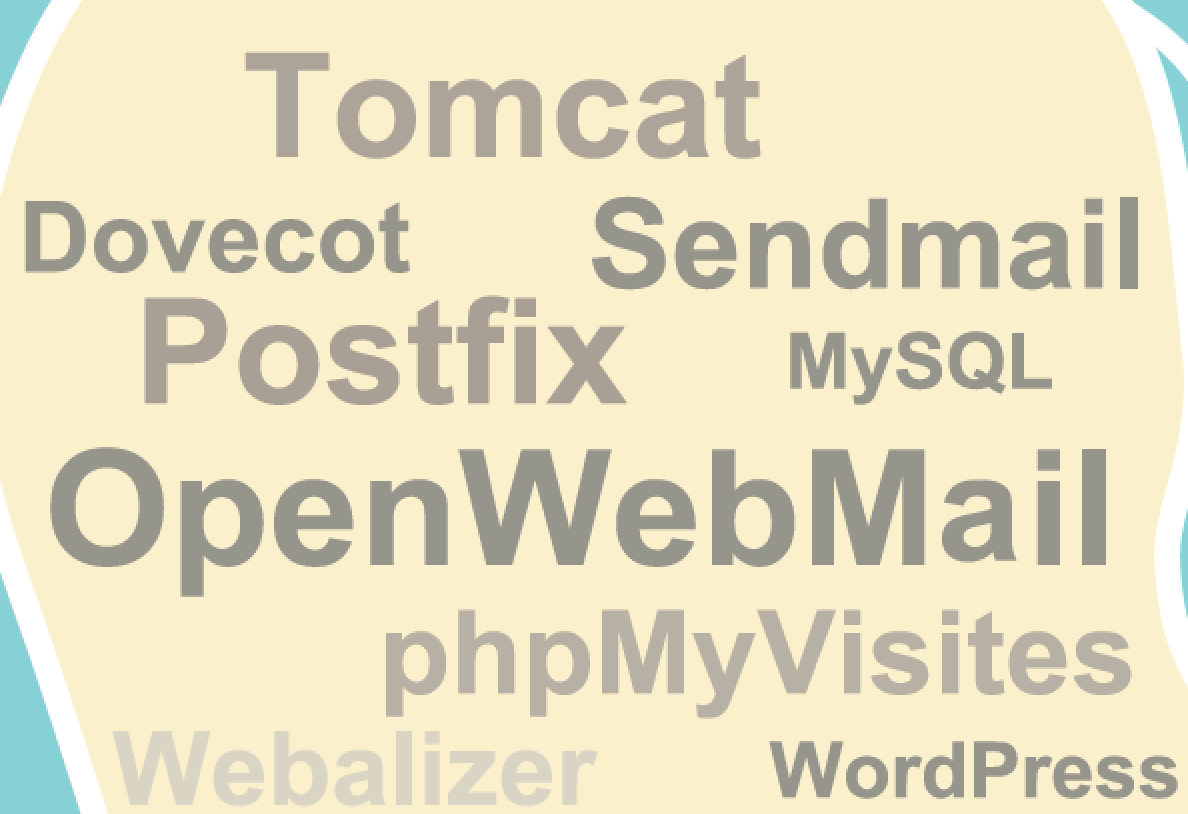



# CentOS 6.x 系统管理




周伯恒 编著

## 全程采用64位环境示范

**最安全** 告诉你如何阻断病毒与垃圾邮件

**最清楚** 完整的步骤解析，跟着做，就搞定

**最详尽** 涵盖服务器配置、流量监控、网站配置

**最热门** 各种邮件服务器、博客、论坛配置，一次搞定




清华大学出版社

# CentOS 6.x 系统管理实战宝典

周伯恒 编著

清华大学出版社
北 京

**本书版权登记号：图字：01-2012-2066**
本书为碁峰资讯股份有限公司授权出版发行的中文简体字版本。

## 内 容 简 介

CentOS 是 Linux 发行版之一，本书全程采用 64 位操作系统进行讲解，内容涉及一般企业 MIS 系统所遇到的服务及错误的处理方法。本书以企业现场实战案例和完整的步骤进行说明，协助读者用最短的时间构建所需的服务，全书共分 6 个部分：基础安装技巧篇，讲解 CentOS 6.X 操作系统的安装和操作使用上的小技巧；服务器配置篇，列举企业常用的服务和服务器配置；邮件服务器篇，讲解如何配置企业内部的邮件服务器；网络流量监控工具篇，详解如何有效地监控网络流量和常见的监控工具应用；LAMP 配置篇，讲述如何配置最稳定的 LAMP 环境；以及附录篇。全书最详尽地涵盖企业各种服务器的配置，如何有效地进行病毒与垃圾邮件的防护，如何最有效地实现流量监控。



**图书在版编目（CIP）数据**

CentOS 6.x 系统管理实战宝典/周伯恒编著. -- 北京 : 清华大学出版社, 2013
ISBN 978-7-302-32340-2

Ⅰ. ①C… Ⅱ. ①周… Ⅲ. ①UNIX 操作系统 Ⅳ.①TP316.81

中国版本图书馆 CIP 数据核字（2013）第 092429 号

**责任编辑：** 夏非彼
**封面设计：** 王　翔
**责任校对：** 闫秀华
**责任印制：**

**出版发行：** 清华大学出版社
**网　　址：** http://www.tup.com.cn，http://www.wqbook.com
**地　　址：** 北京清华大学学研大厦 A 座　　**邮　　编：** 100084
**社 总 机：** 010-62770175　　**邮　　购：** 010-62786544
**投稿与读者服务：** 010-62776969，c-service@tup.tsinghua.edu.cn
**质量反馈：** 010-62772015，zhiliang@tup.tsinghua.edu.cn

**印 装 者：**
**经　　销：** 全国新华书店
**开　　本：** 190mm×260mm　　**印　　张：** 27　　**字　　数：** 691 千字
**版　　次：** 2013 年 0 月第 1 版　　**印　　次：** 2013 年 0 月第 1 次印刷
**印　　数：** 1~3500 册
**定　　价：** 59.00 元

---

产品编号：047309-01

# 前　言

当前企业的IT应用环境是一种混杂模式，就操作系统而言，除Windows之外开源操作系统在关键应用领域一直处于核心地位。特别是Linux操作系统，已经成为了未来发展的趋势。究其原因，与Linux操作系统的理念相关。Linux操作系统提倡免费、开源的理念，这有利于企业能够更好地控制IT成本，更灵活地利用操作系统。在众多的Linux发行版中Red Hat Linux是最受企业欢迎的Linux发行版之一，但是使用该发行版会涉及购买支持服务的问题。CentOS操作系统作为Red Hat Linux操作系统的释出版本是没有任何使用费用的，性能上与Red Hat Enterprise Linux差异较小，功能结构与Red Hat Linux几乎相同，使用与Red Hat Enterprise Linux类似。该操作系统分为32位及64位，因为近几年的处理器以64位为主，连Windows Server 2008 R2都抛弃了32位操作系统，当然就要选择64位的操作系统。

本书内容分为6个篇章，笔者全程以64位的CentOS 6.x进行介绍，内容以一般企业MIS所遇到的服务及错误进行介绍，希望大家使用CentOS时更容易上手。本书没有讨论太多理论，而是直接介绍如何在最短的时间内构建所要的服务，所以若是要深入了解的话，可以参考其他书籍。本书所有步骤都经笔者测试，由于内容很多，若有缺漏请读者批评指正。

Jerry_IT 周伯恒

# 目　录

## 第一部分　基础安装技巧篇

# 第二部分 服务器配置篇

# 第三部分 邮件服务器篇

# 第四部分 网络流量监控工具篇

# 第五部分 LAMP配置篇

# 第六部分　附录篇

# 第一部分

# 基础安装技巧篇

# 第 1 章

# CentOS系统安装介绍

CentOS官方网站：http://www.centos.org/ 。

CentOS（Community ENTerprise Operating System）是Linux发行版之一，它是来自于Red Hat Enterprise Linux依照开放源代码规定释出的源代码所编译而成。由于出自同样的源代码，因此有些要求高度稳定性的服务器以CentOS替代商业版的Red Hat Enterprise Linux使用。两者的不同，在于CentOS并不包含非开源源代码软件。

## 1.1 CentOS操作系统下载

官方提供了所有CentOS操作系统版本下载，可根据需求下载所需的操作系统版本，本书介绍的是CentOS 6.0 x86_64版本。

| 官方 CentOS 版本下载 | | |
|---|---|---|
| CentOS 6 | i386 | http://isoredirect.centos.org/centos/6/isos/i386/ |
| | x86_64 | http://isoredirect.centos.org/centos/6/isos/x86_64/ |
| CentOS 5 | i386 | http://isoredirect.centos.org/centos/5/isos/i386/ |
| | x86_64 | http://isoredirect.centos.org/centos/5/isos/x86_64/ |
| CentOS 4 | i386 | http://isoredirect.centos.org/centos/4/isos/i386/ |
| | x86_64 | http://isoredirect.centos.org/centos/4/isos/x86_64/ |
| CentOS 3 | i386 | http://isoredirect.centos.org/centos/3/isos/i386/ |
| | x86_64 | http://isoredirect.centos.org/centos/3/isos/x86_64/ |

下面列举几个中国台湾地区学校较为知名的文件服务器，这些服务器更新速度比较快，下载路径在CentOS目录内，有x86_64和i386版本可供下载。

| 学校名称 | 下载路径 |
|---|---|
| 义守大学 | http://ftp.isu.edu.tw/pub/Linux/CentOS |
| 中山大学 | http://ftp.nsysu.edu.tw/CentOS/ |
| 中兴大学 | http://ftp.nchu.edu.tw/Linux/CentOS/ |

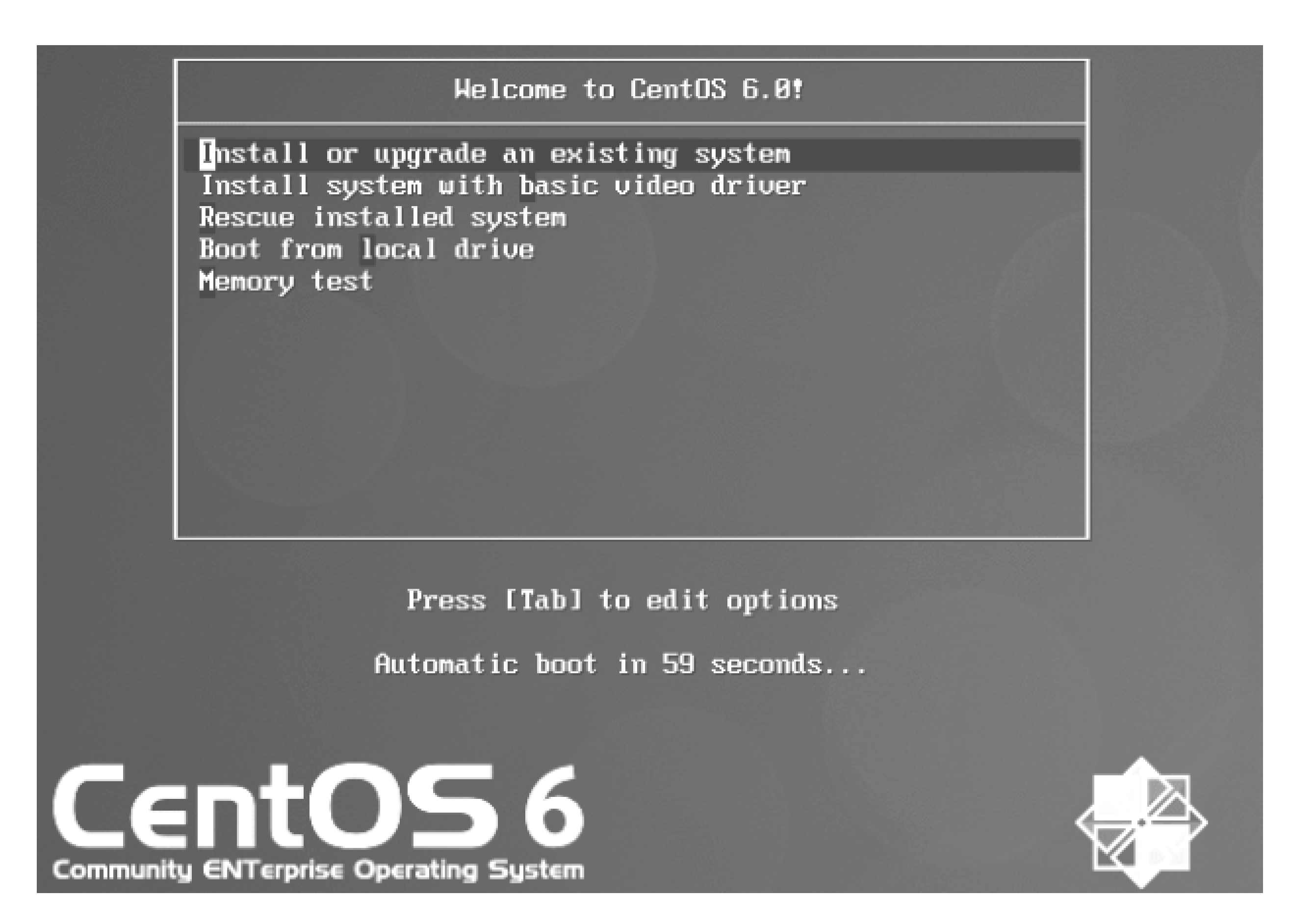
（续表）

| 学校名称 | 下载路径 |
| --- | --- |
| 淡江大学 | http://ftp.tku.edu.tw/index.php?dir=Linux%2FCentOS%2F |
| 亚洲大学 | http://ftp.asia.edu.tw/ftp/index.php?dir=%2FOS%2FLinux/CentOS |
| 昆山科技大学 | http://ftp.ksu.edu.tw/FTP/CentOS/ |

## 1.2 CentOS操作系统光盘安装方法

CentOS安装方法越来越简单，比起以往的Red Hat已经很好安装了，安装方法的简单性可比Windows操作系统。以下安装语言为简体中文，是为了方便了解配置，不过建议选择英文语言安装，以便在后面的操作中避免一些不必要的错误，若要安装简体中文当然也没关系。

步骤01 操作系统安装选项。在CentOS 6.x安装欢迎界面中选择【Install or upgrade an existing system】进行安装，如果没有选择，系统60秒后也会自动以此模式进行安装。



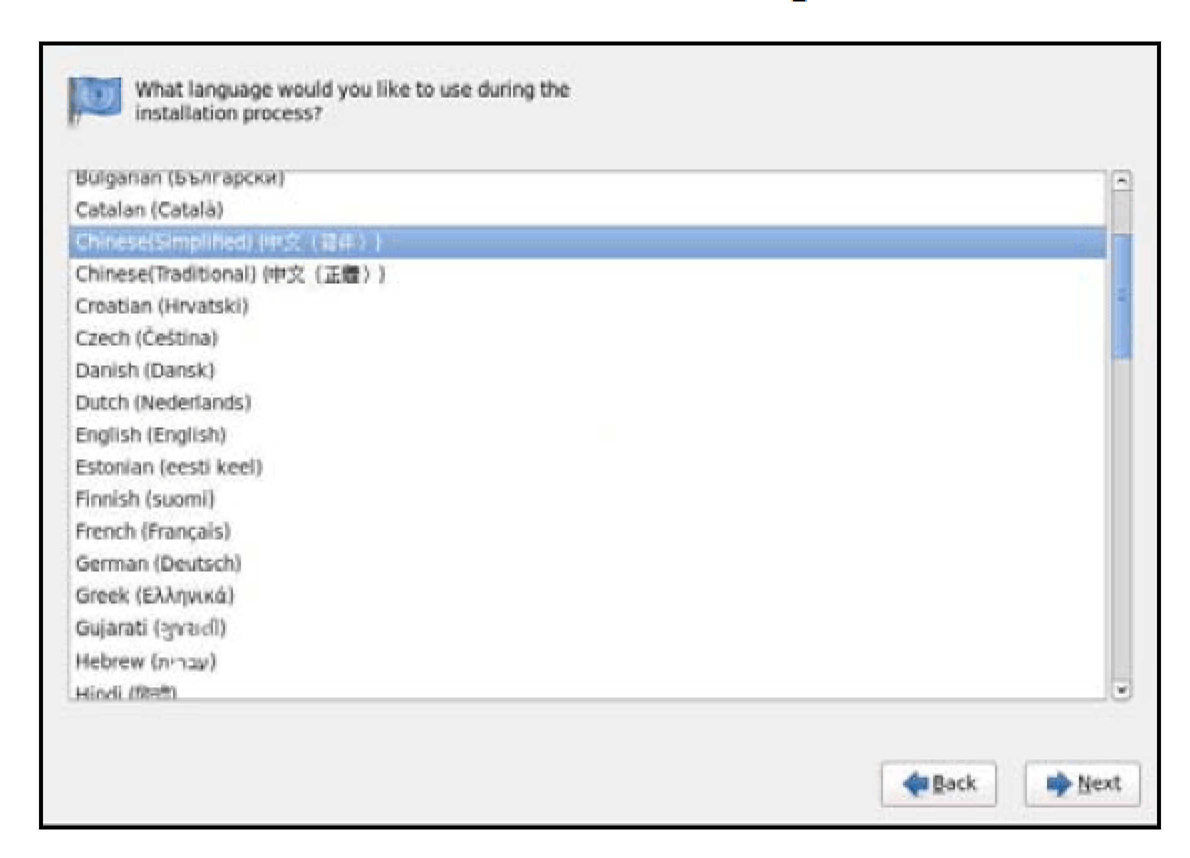

步骤02 安装前检查光盘。检查光盘的作用就是避免安装来源文件有问题，导致安装失败，以往是CD-R时，会有多张光盘，在安装过程中若其中一张光盘损坏，那就是浪费时间，而现在使用DVD光盘或在虚拟机下使用ISO文件安装，这个检查就比较多余，所以确定安装来源没问题，可以选择【Skip】略过检查。



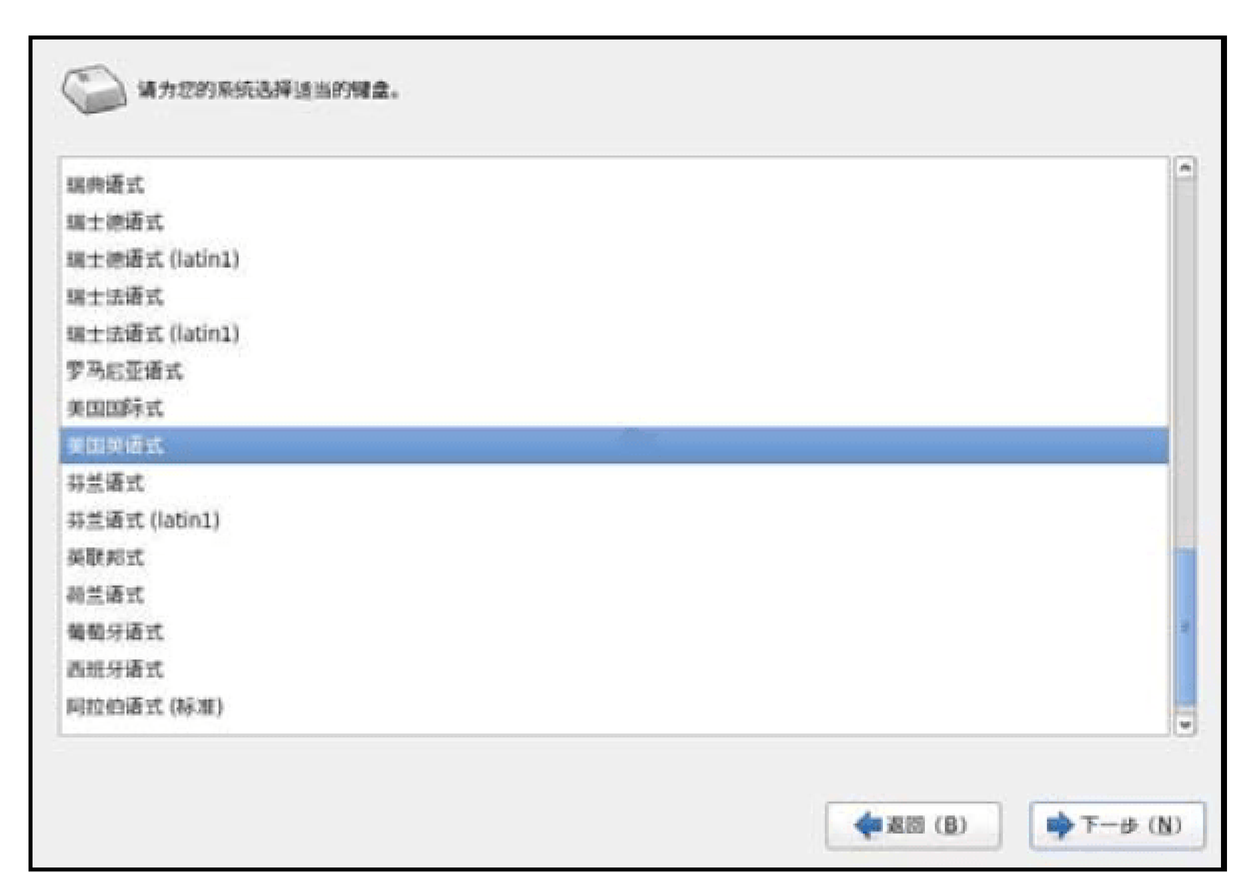

步骤03 在CentOS安装欢迎画面中，按【Next】。



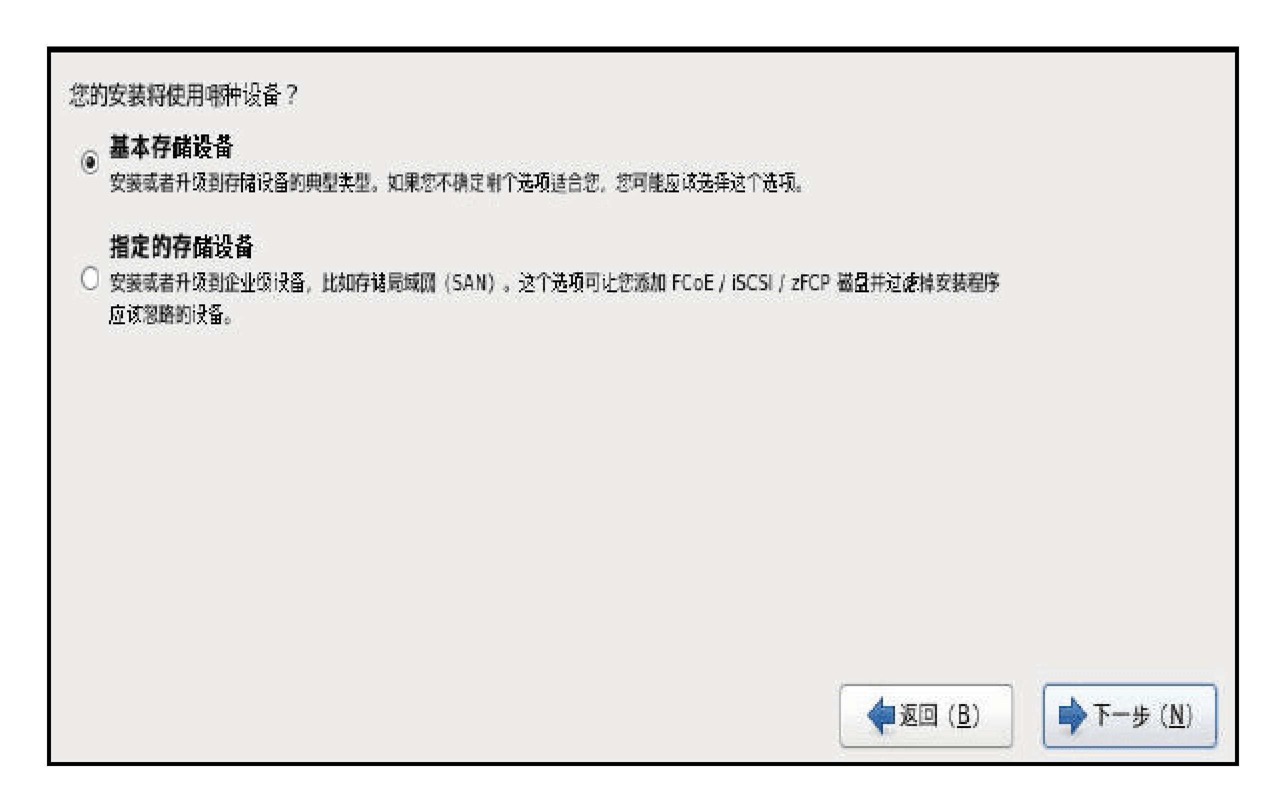

步骤04　选择操作系统语言。选择【Chinese(Simplified)(中文(简体))】后，按【Next】。




步骤05　选择系统的键盘。选择【美国英语式】，按【下一步】。




步骤06　选择安装的磁盘类型。一般选择【基本储存设备】，除非有其他的储存设备，如SAN等企业级储存设备，选择完毕后，按【下一步】。




步骤07 系统要写入信息时会产生警告信息，此警告信息是说若要进行全新的硬盘安装，必须要重新初始化，按【重新初始化所有】。




步骤08 配置主机名称。默认名称为localhost.localdomain，若目前没有想要配置的名称及域名，可以安装完后再进行配置，按【下一步】。



**说明**

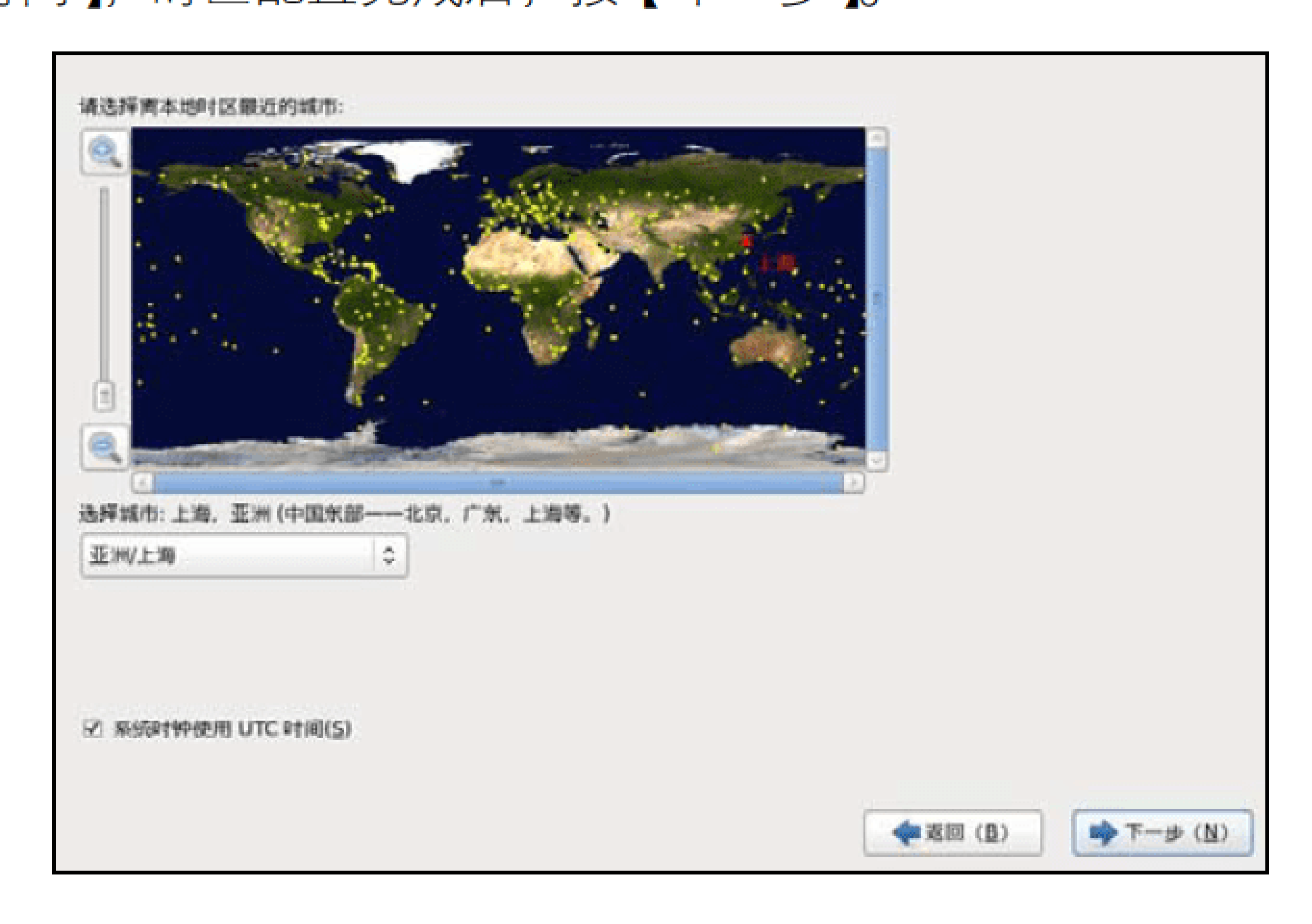
由于CentOS 6.x安装好后，默认不会自动进行网络连接，所以在安装过程中，可勾选自动连接，否则只能安装完后再开启。按【配置网络】，在网络连接窗口中选择网络适配器：System eth0，按【编辑】。




在编辑窗口中勾选【自动连接】，再按【应用】→【关闭】，当操作系统安装完毕后，就会自动启动网络适配器。

正在编辑 System eth0
连接名称(I) System eth0
自动连接(A)
有线 | 802.1x 安全性 | IPv4 设置 | IPv6 设置
设备 MAC 地址(D)： 00:0C:29:3E:A6:E0
克隆 MAC 地址(C)：
MTU： 自动 字节

**步骤 09** 配置时区。系统会以你选择的语言判断你的时区，目前选择为简体中文，所以城市为【亚洲/上海】，若是选择英语语系则为美国，要勾选【系统时钟使用UTC时间】，时区配置完成后，按【下一步】。



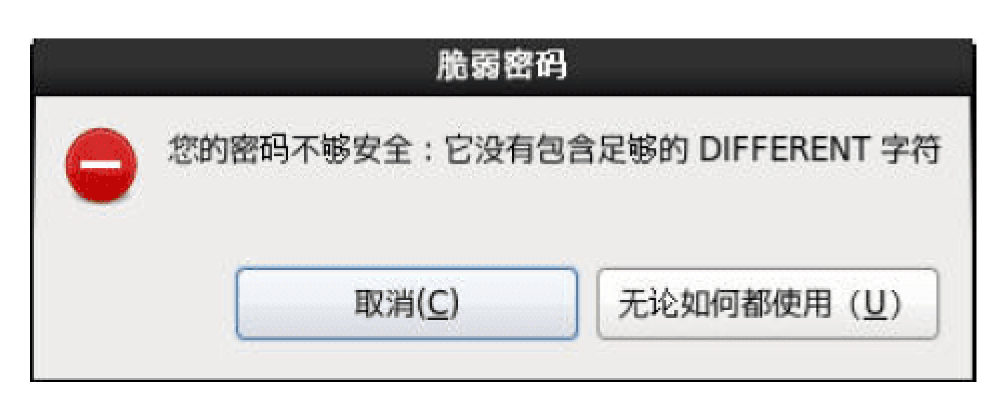

**说明**

UTC为世界标准时间，中国时区为UTC+8。

步骤 10 设置系统管理员root账号的密码。所要设置的密码需输入两次，设置完成后，按【下一步】。




步骤 11 若输入的密码不符合密码复杂度，系统则会警告密码不够安全，按【取消】会回到上一步重新输入密码，或按【无论如何都使用】继续使用目前所设置的密码。



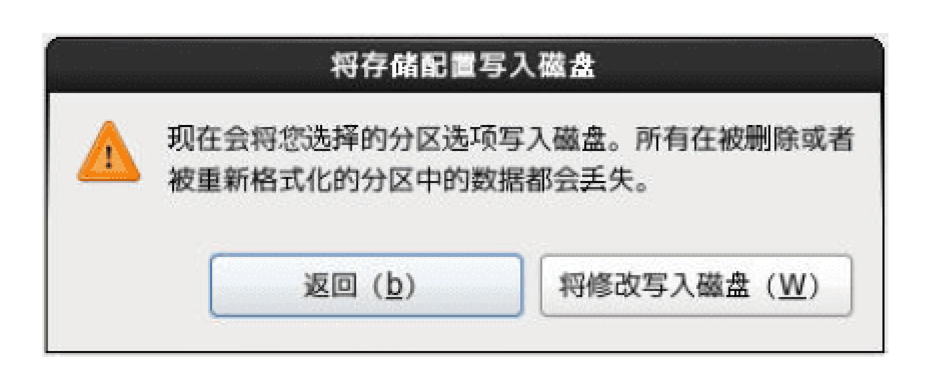

步骤 12 选择要以哪种类型安装。现在为全新安装的硬盘，没有安装其他的操作系统，所以选择【替换现有Linux系统】。若有其他分区需求，则可以选择【创建自定义布局】，甚至可以勾选【查看并修改分区布局】，来查看目前选择类型的分区方法，按【下一步】。




- 使用所有空间（Use All Space）：此方法会删除所选择硬盘上的所有分区（包括其他操作系统创建的分区），然后再重新对硬盘分区。如果硬盘上有想保留的操作系统或数据，请不要选择此项。

- 替换现有Linux系统（Replace Existing Linux System）：此方法只删除硬盘上所有GNU/Linux分区，然后再重新对硬盘分区。此方法不会删除其他操作系统的分区，包括Windows系统的NTFS和FAT32等。如果硬盘上有想保留的GNU/Linux系统或里面有重要数据，请不要选择此项。
- 缩小现有系统（Shrink Current System）：如果整个硬盘已有一个分区（多数为Windows的NTFS分区或FAT分区），就会看到这个方法。此方法会在不损害原有分区数据（不影响Windows系统）的情况下缩小分区，并在腾出的空间上安装CentOS。
- 使用剩余空间（Use Free Space）：此方法不会删除任何分区，只使用尚未分给任何分区的空间进行自动分区。当然如果硬盘早已被另一个操作系统占用了，此项根本用不了。
- 创建自定义布局（Create Custom Layout）：此方法不会自动分区，而是执行一个叫Disk Druid的程序，以手动创建硬盘分区。

步骤13 系统会将磁盘分区配置写入磁盘，写入前会有确认提示，确认无误后，按【将修改写入磁盘】。




步骤14 选择安装服务类型，CentOS 6.x列出了几种安装模式。一般来说CentOS都是应用在Server上，很少使用Desktop，Server默认不会安装图形界面，只有Desktop才有。除了VNC Server，后面介绍的均为服务器配置应用，所以建议选择【Basic Server】服务器基本安装，这样以后安装服务时，就可以了解服务所需的软件，可以了解系统的应用。选择完毕后，如果要安装其他软件，可以选择【现在自定义】，否则直接保留默认的【以后自定义】，接下来按【下一步】安装CentOS 6.x操作系统。

- 桌面（Desktop）：使用GNOME的桌面环境。
- 最小的桌面（Minimal Desktop）：只提供运行图形桌面必要的最基本软件。
- 最小的（Minimal）：只提供运行GNU/Linux必要的最基本软件。
- 基本服务器（Basic Server）：基本服务器软件。
- 数据库服务器（Database Server）：使用MySQL和PostgreSQL服务器软件。
- 网站服务器（Web Server）：使用Apache网站服务器。
- 企业身份识别服务器（Enterprise Identity Server Base）：提供OpenLDAP和the System Security Services Daemon（SSSD）等，主要是建立身份识别和确认身份的服务器。
- 虚拟化系统（Virtual Host）：有关支持虚拟化的软件，包括KVM、Virtual Machine Manager、VM版面程序。
- 软件开发工作站（Software Development Workstation）：提供软件开发。




步骤15 CentOS 6.x操作系统开始安装，安装时间大概半个小时。




步骤16 CentOS 6.x操作系统安装完成，按【重新引导】。




步骤17 由于选择了Basic Server（基本服务器）安装，所以没有任何图形界面，输入root账号和密码后，即可以进入操作系统。

```
CentOS Linux release 6.0 (Final)
Kernel 2.6.32-71.el6.x86_64 on an x86_64

localhost login:
```

# 1.3 CentOS操作系统网络安装方法

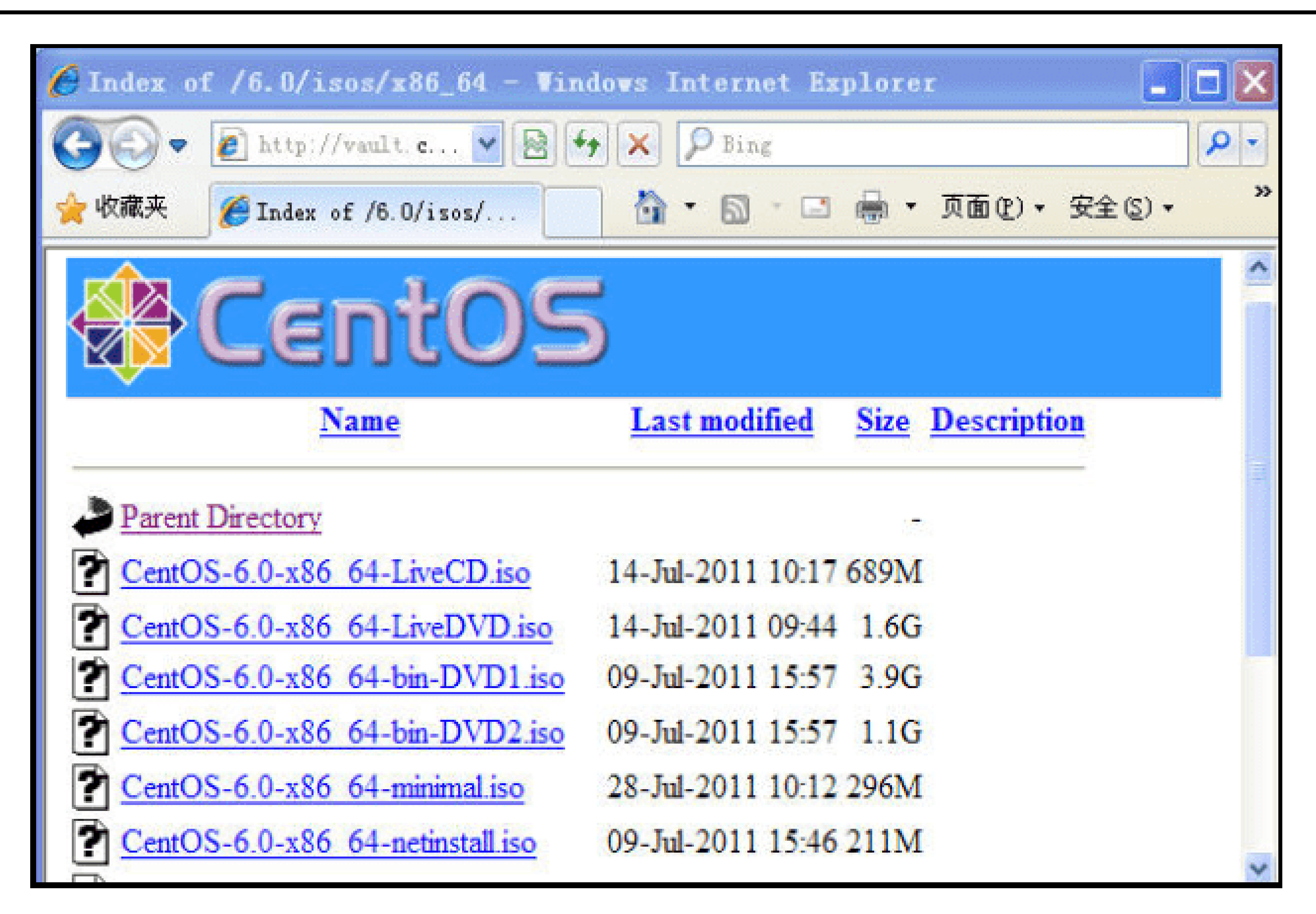
安装CentOS 6.x操作系统除了使用光盘方法安装外，还可以使用网络方法安装，不过安装的服务器类型不同，操作系统的容量也不太一样。若安装的服务器类型容量很大，就不建议使用网络方法安装，以免浪费太多带宽。前面的章节已经介绍过怎样安装CentOS 6.x操作系统，所以后面对此不再赘述，只告诉大家如何使用CentOS 6.x网络安装版安装，只需要指定网络安装文件的来源，接下来的安装步骤和光盘安装方法相同。

## 下载CentOS网络安装文件

安装CentOS 6.x前，曾介绍过从哪里获得CentOS 6.x网络安装版光盘，与CentOS光盘安装版一样，从最常使用的CentOS官方文件服务器下载，速度快又稳定，也可以选择适合自己的文件服务器或官方网站下载。

目前最新版为6.0版本，以下列出了x86_64和i386版本，不过建议使用x86_64，后面的介绍都会以64位的操作系统进行配置。

| | |
|---|---|
| x86_64 | http://vault.centos.org/6.0/isos/x86_64/CentOS-6.0-x86_64-netinstall.iso |
| i386 | http://vault.centos.org/6.0/isos/i386/CentOS-6.0-i386-netinstall.iso |




下载好CentOS 6.x网络安装版后，将镜像文件刻录成光盘，或者使用虚拟化软件挂载镜像文件安装。启动电源，配置BIOS以光盘开机引导CentOS 6.x操作系统进行网络安装。

步骤01 CentOS 6.x操作系统安装选项与一般光盘安装选项相同，选择【Install or upgrade an existing system】，然后按【Enter】，若不选择，系统60秒后也会自动以此模式进入安装。



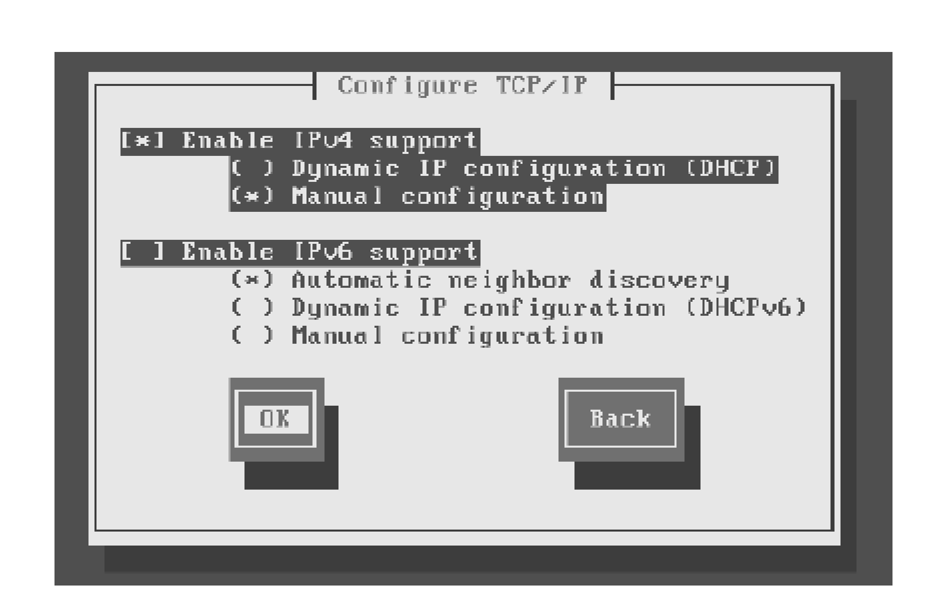

步骤02　安装前检查光盘。检查光盘的作用就是避免安装来源文件有问题，导致安装失败，不过网络安装来源只有一张光盘，所以失败的机率就比较小，可直接选择【Skip】略过光盘检查。



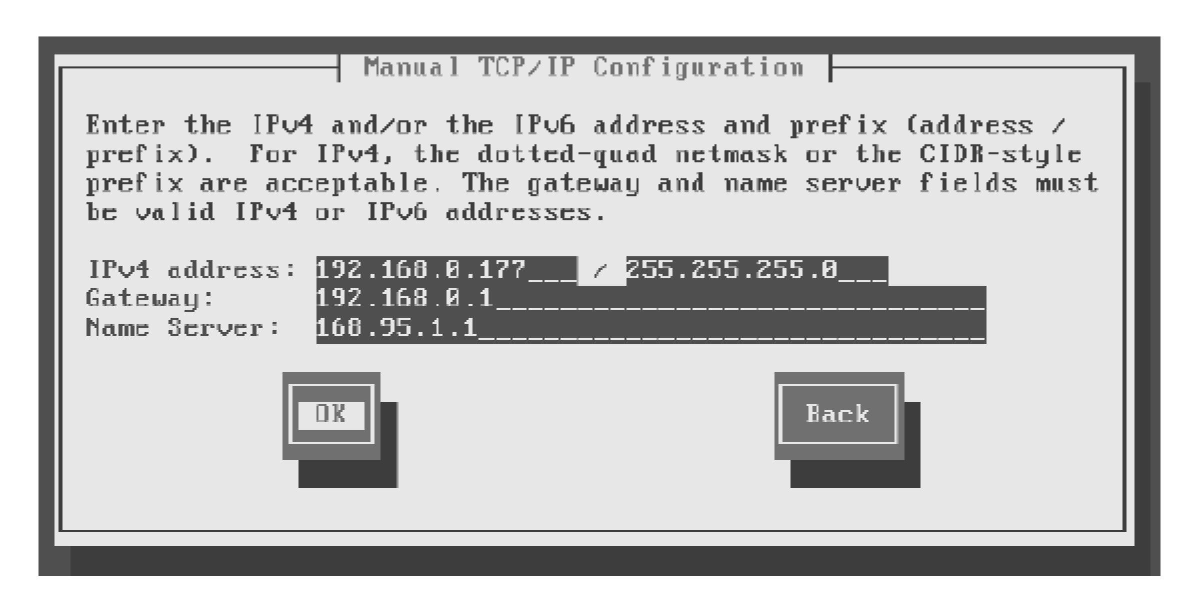

步骤03　选择安装方法。由于是CentOS 6.x网络安装版，所以会问要以哪种方法安装，请选择【URL】网络方法安装，选择完毕后，按【OK】。




步骤04　进行网络安装前一定需要网络才可以安装，所以必须要配置网络，否则无法继续安装。网络配置支持IPv4和IPv6两种协议，大多环境使用IPv4协议，这里示范IPv4协议的固定IP地址配置，若环境是DHCP服务器，则可以选择【Dynamic IP configuration（DHCP）】，若是固定IP地址，则选择【Manual configuration】。没有使用IPv6协议的话，记得要取消选择，以免安装失败，选择完毕后，按【OK】。




步骤05 网络配置方法很简单，就是配置IP地址、子网掩码（subnet）、网关（Gateway）和域名服务器（DNS，Name Server），配置完成后，按【OK】。



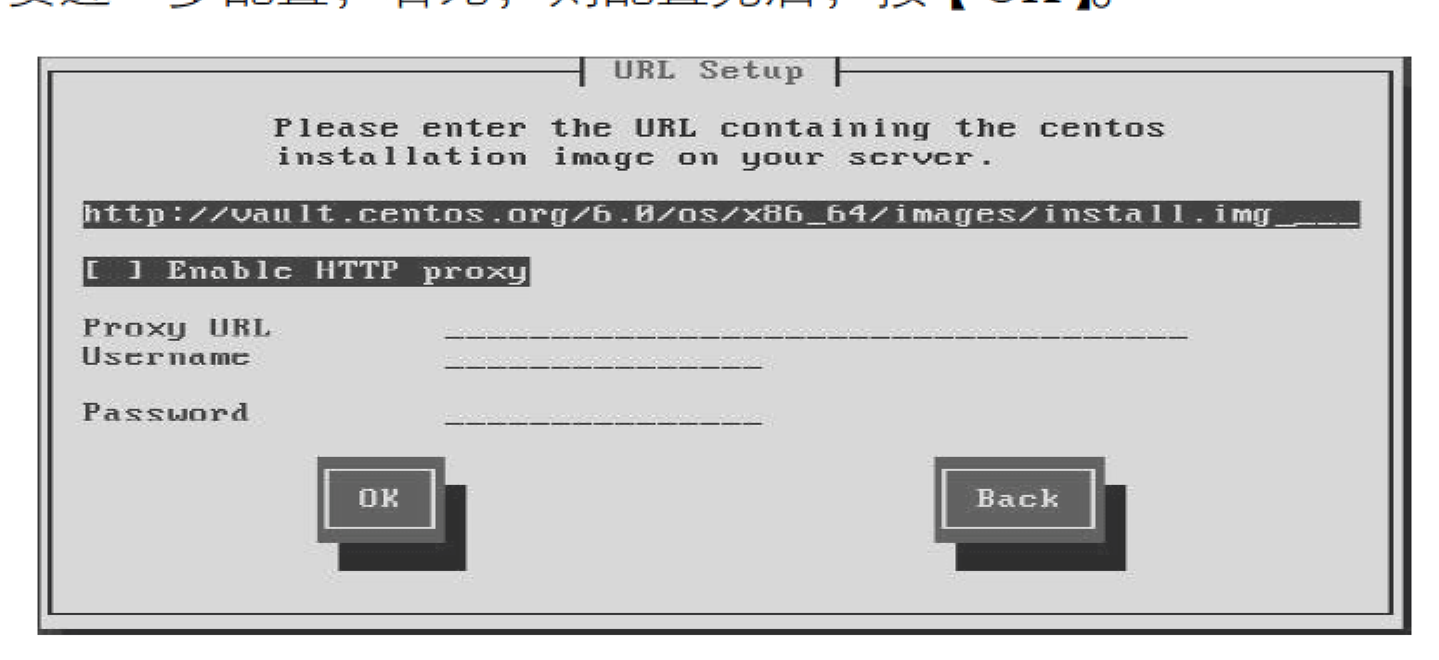

步骤06 系统会配置并检查eth0网络是否正常。




**说明**

eth0为系统的第一个网络适配器。

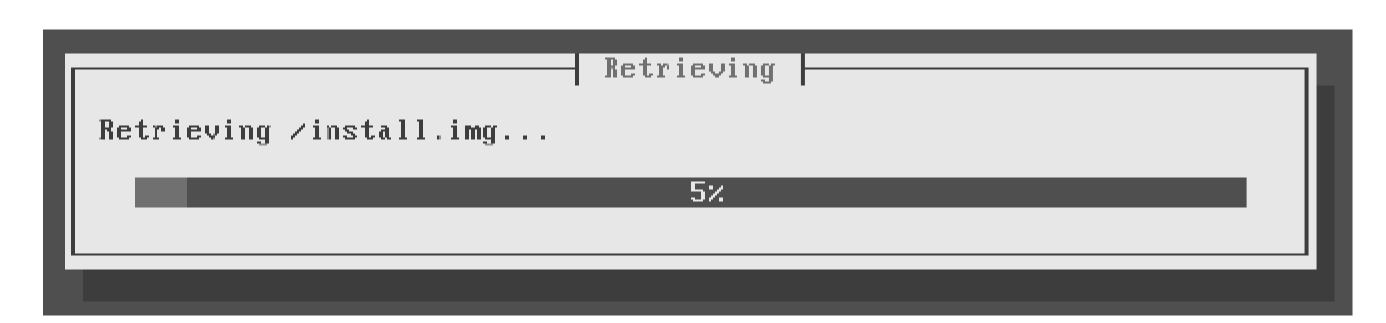
步骤07 配置安装文件来源。输入安装来源路径，这里安装CentOS 6.0 x86_64的路径为：http://vault.centos.org/6.0/os/x86_64/images/ install.img。若需要代理服务器才需要进一步配置，若无，则配置完后，按【OK】。




此处采用CentOS文件服务器来当作安装文件来源，有CentOS的x86_64和i386版本，可根据需求选择。目前版本为6.0版，如果有新版本，基本上改掉版本号应该可以，或者可以到该文件服务器上查询最新路径。

| 版本 | 安装来源路径 |
|---|---|
| x86_64 | http://vault.centos.org/6.0/os/x86_64/images/install.img |
| I386 | http://vault.centos.org/6.0/ os/i386/images/install.img |

步骤08 CentOS 6.0安装程序会检测所配置的安装来源，若安装来源路径错误则会回到上一步，若安装来源路径正确，则会进入CentOS 6.x操作系统的安装。




步骤09 CentOS 6.x操作系统安装主界面。这样就代表安装来源路径正确，可以开始进行安装。后续的操作与光盘安装方法相同，只要注意安装过程中，网络不可以中断，以免安装失败，安装速度则会因环境不同而不同。




# 1.4 安装后的必要配置

CentOS 6.x操作系统安装完成，重新启动后，有很多配置需要修改，不过最重要的就是关闭SELinux。SELinux是增强安全性的一项功能，CentOS 6.x操作系统默认启动。为什么要关闭呢？不是SELinux功能不好，而是当功能安全性较高时，会带来很多不便，为了初学者或管理者使用方便，大多都会将此配置关闭，所以在CentOS 6.x操作系统安装完成后，最好马上就关闭SELinux，以免事后安装或配置其他服务时，发生不必要的错误与困扰。关闭的方法很简单，编辑SELinux配置文件，将配置设为disabled。完成后必须要重新启动，配置才会生效。输入【shutdown -r now】。

```
[root@localhost ~]# vi /etc/sysconfig/selinux    //编辑 SELinux 配置文件
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
```

```
#     disabled - No SELinux policy is loaded.
SELINUX=disabled                                //disabled 为关闭 SELinux
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

# 第 2 章

# 网络应用配置

## 2.1 配置网络IP地址

CentOS操作系统的网络配置方法分为文本模式和图形模式，不管用哪种方法，从CentOS 6.x版本之后，都要使用文本模式将网卡配置参数ONBOOT设为yes，如果使用默认的no，即使网络配置完成，也无法成功连接网络。

### 使用文本模式配置网络

先到网卡配置文件目录位置，可以看到目前网卡的配置文件，第一块网卡的配置文件名称为ifcfg-eth0，第二块网卡为ifcfg-eth1，后面依此类推。

```
[root@localhost ~]# cd /etc/sysconfig/network-scripts
                           //网卡配置文件目录
[root@localhost network-scripts]# ls
                           //查看配置文件，默认第一块网卡名称为 ifcfg-eth0
ifcfg-eth0   ifdown-isdn    ifup-aliases  ifup-plusb     init.ipv6-global
ifcfg-lo     ifdown-post    ifup-bnep     ifup-post      net.hotplug
ifdown       ifdown-ppp     ifup-eth      ifup-ppp       network-functions
ifdown-bnep  ifdown-routes  ifup-ippp     ifup-routes    network-functions-ipv6
ifdown-eth   ifdown-sit     ifup-ipv6     ifup-sit
ifdown-ippp  ifdown-tunnel  ifup-isdn     ifup-tunnel
ifdown-ipv6  ifup           ifup-plip     ifup-wireless
```

编辑第一块网卡配置文件，CentOS 6.x网卡配置文件与之前版本的配置文件略微不同，以下分别是DHCP自动获取IP配置方法及固定IP地址配置方法。注意：CentOS 6.x网卡配置文件内ONBOOT参数默认为no，必须要自行修改为yes，否则通过命令工具配置IP地址后，也不能使用。

```
DHCP 自动获取 IP 配置方法
[root@localhost network-scripts]# vi ifcfg-eth0
                              //编辑网卡配置文件
DEVICE=eth0                   //网卡设备名称为 eth0，依此类推
HWADDR=00:50:56:81:00:15      //网卡设备 MAC 地址，每个 MAC 地址独一无二
ONBOOT=yes                    //CentOS 6 默认为 no（不启用），以前版本默认为 yes（启用），
                                所以必须配置为 yes（启用）
BOOTPROTO=dhcp                //CentOS 6 的第一块网卡配置文件中无此行，必须手工添加，
                                第二块网卡配置文件则有，以前版本为 DHCP 模式
固定 IP 地址配置方法
[root@localhost network-scripts]# vi ifcfg-eth0
                             //编辑第一块网卡配置文件
DEVICE=eth0                  //网卡设备名称为 eth0，依此类推
HWADDR=00:50:56:81:00:15     //网卡设备 MAC 地址，每个 MAC 地址独一无二
NM_CONTROLLED=yes
ONBOOT=yes                   //CentOS 6 默认为 no（不启用），以前版本默认为 yes（启用），
                               所以必须配置为 yes（启用）
IPADDR=192.168.233.229       //网络 IP 地址
BOOTPROTO=none               //CentOS 6 的第一块网卡配置文件中无此行，必须手工添加，
                               第二块网卡配置文件则有，以前版本为 DHCP 模式
NETMASK=255.255.255.0        //子网掩码
TYPE=Ethernet                //网络类型
GATEWAY=192.168.233.254      //网关
DNS1=168.95.1.1              //名称解析服务器，此配置也可以在 resolv.conf 中编辑
IPV6INIT=no                  //不使用 IPV6INIT
```

固定IP地址配置方法除了配置网络外，还要配置DNS服务器。在etc目录下，修改resolv.conf配置文件，编辑所要配置的DNS服务器，如果在网卡配置文件中就有配置DNS服务器信息的话，resolv.conf中就会有DNS配置信息。

```
[root@localhost ~]# vi /etc/resolv.conf      //编辑 DNS 配置文件
nameserver 168.95.1.1                        //第一台 DNS 服务器，依此类推
```

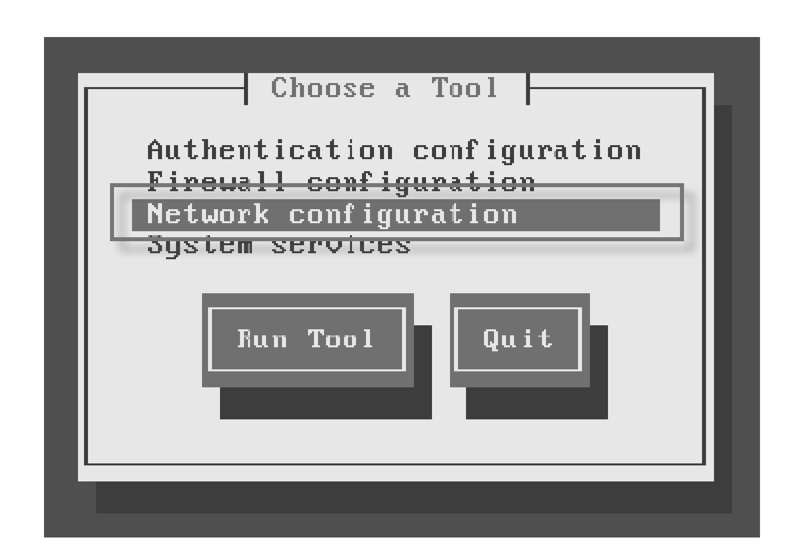
编辑完网卡配置文件及DNS配置文件后，必须重新启动网络服务才会生效。

```
[root@localhost network-scripts]# service network restart
Shutting down interface eth0:                          [  OK  ]
Shutting down loopback interface:                      [  OK  ]
Bringing up loopback interface:                        [  OK  ]
Bringing up interface eth0:                            [  OK  ]
```

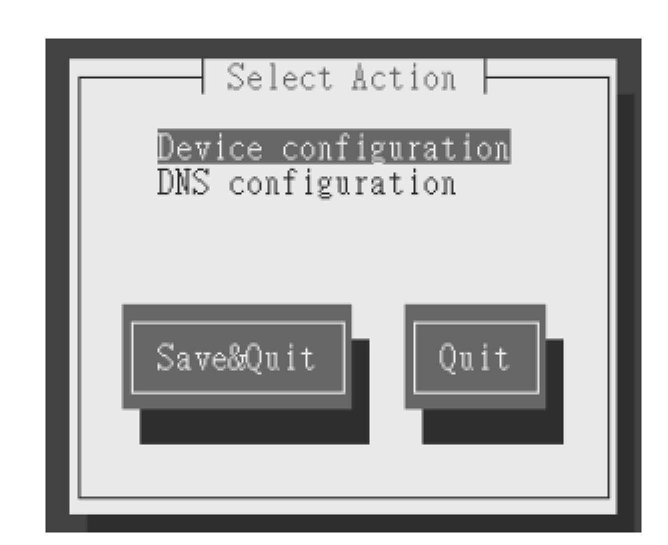
## 使用图形方法配置网络

Choose a Tool是一种非常方便的配置工具，无需输入长长的命令，只要几个操作就可以完成，但是此工具在putty远程连接工具中可能会无法开启，建议在本机中配置。Choose a Tool在CentOS 6.x最小安装模式中是没有安装的，必须手动安装。

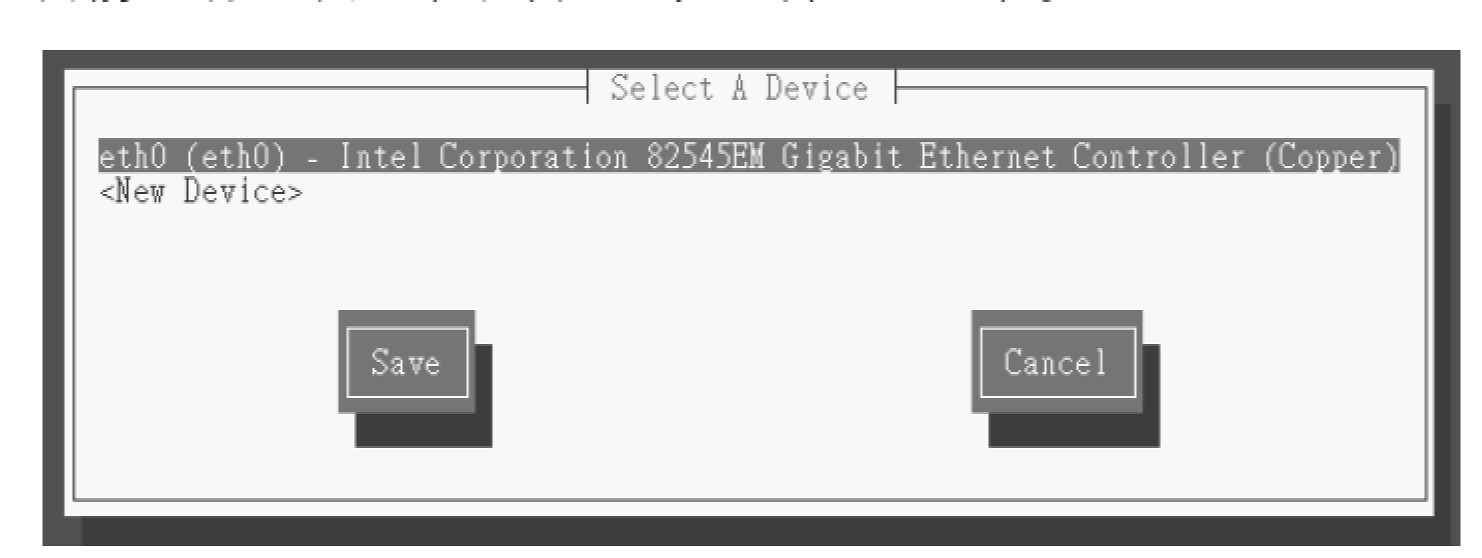
步骤01 使用Choose a Tool工具修改，在文本模式中输入【setup】即可开启进入，选择【Network configuration】，按【Run Tool】。



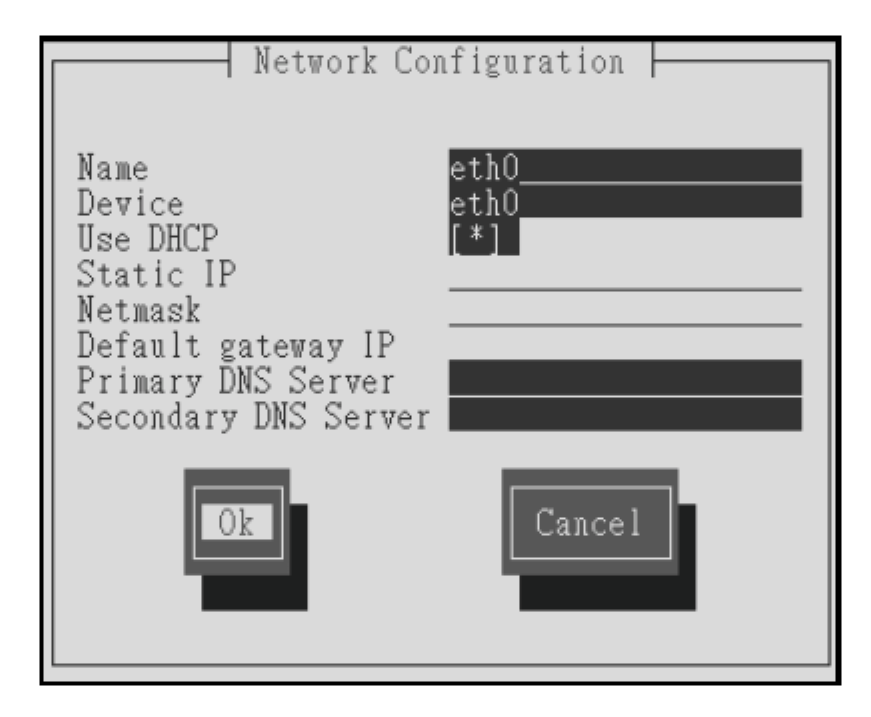

步骤02 选择【Device configuration】。



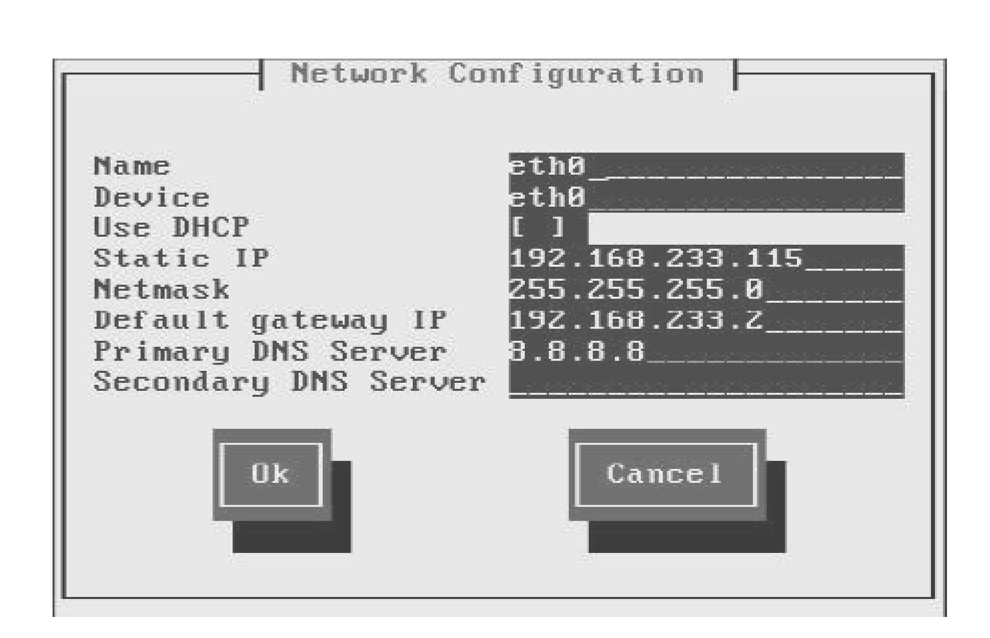

步骤03 目前只有一块网卡设备eth0，选择eth0网卡。




步骤04 默认为DHCP模式，如果网络是使用DHCP配置IP地址就无需修改。



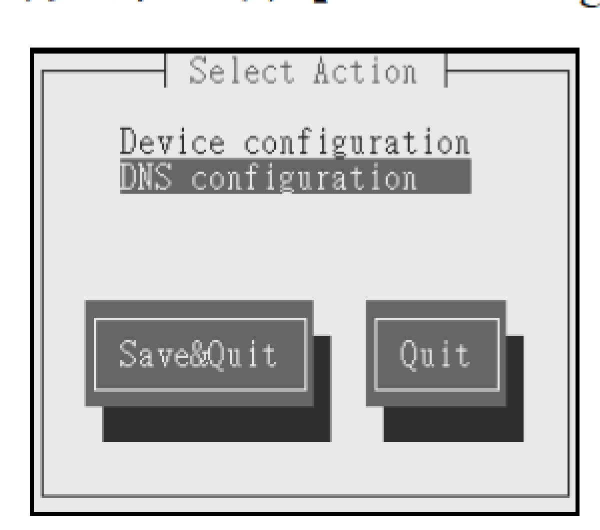

步骤05 配置固定IP地址必须先将【Use DCHP】选项取消，配置好IP地址后，按【Ok】。CentOS 6.x比以往的版本多了DNS服务器配置，所以如果有配置则会同步到DNS配置文件（resolv.conf）中。




步骤 06 网络配置完成，按【Save】保存。



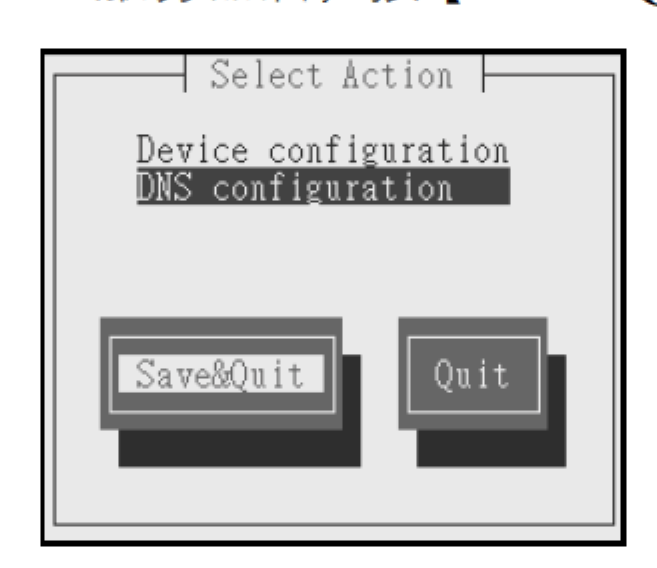

步骤 07 接下来配置DNS服务器，选择【DNS configuration】。




步骤 08 配置计算机名称及DNS服务器，配置完成后，按【Ok】离开。




步骤 09 配置完IP地址及DNS服务器后，按【Save&Quit】，保存并退出。



步骤10 按【Quit】，退出Choose a Tool。




步骤11 网络配置完成后，必须重新启动网络服务，配置信息才会生效。

```
[root@localhost ~]# service network restart
Shutting down interface eth0:                               [  OK  ]
Shutting down loopback interface:                           [  OK  ]
Bringing up loopback interface:                             [  OK  ]
Bringing up interface eth0:                                 [  OK  ]
```

## 2.2 主机禁止ping

Ping命令在网络检测中是最常用的一个命令，所用的就是ICMP协议，不过为了保护主机，通常会禁用ICMP协议，忽略ICMP数据包，再使用ping方法对这台主机检测，这时没有任何反应。

### 禁用ICMP协议

若要禁用ICMP协议，可以直接输入参数或编辑配置文件，配置完成后无需重新启动。

```
[root@localhost ~]#echo "1" >/proc/sys/net/ipv4/icmp_echo_ignore_all
                                  //直接输入参数
[root@localhost ~]#vi /proc/sys/net/ipv4/icmp_echo_ignore_all
1                                 //1 为禁用，默认没有配置，表示启用 ICMP 协议
```

再使用其他主机去ping该主机，会出现请求超时信息。

```
C:\Documents and Settings\user>ping 192.168.233.229
Pinging 192.168.233.229 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

### 启用ICMP协议

若要启用ICMP协议，可以直接输入参数或编辑配置文件，配置完成后无需重新启动。

```
[root@localhost ~]# echo "0" >/proc/sys/net/ipv4/icmp_echo_ignore_all
                                  //直接输入参数
[root@localhost ipv4]# vi /proc/sys/net/ipv4/icmp_echo_ignore_all
0                                 //0 为启用，默认没有配置，表示启用 ICMP 协议
```

再使用其他主机去ping该主机，就会有回复的信息。

```
C:\Documents and Settings\user>ping 192.168.233.229
Pinging 192.168.233.229 with 32 bytes of data:
Reply from 192.168.233.229: bytes=32 time=19ms TTL=62
Reply from 192.168.233.229: bytes=32 time=1ms TTL=62
Reply from 192.168.233.229: bytes=32 time=1ms TTL=62
```

## 2.3 单一网卡配置多个IP地址

一般来说网卡在CentOS操作系统中可以配置多个IP地址，如果要配置两个IP地址不一定要有两块网卡，两个IP地址可以共享一块网卡设备，是否要配置多个IP地址可根据实际情况决定。

查看网卡信息，第一个网卡设备名称为eth0，表示只有一块网卡，如果有第二块网卡就叫做eth1，lo是本机local loopback，建议不要随意修改lo配置，目前使用的IP地址为192.168.233.229。

```
[root@localhost ~]#ifconfig    //查看网卡信息
eth0    Link encap:Ethernet  HWaddr 00:50:56:81:00:15
        inet addr:192.168.233.229  Bcast:192.168.233.255 Mask:255.255.255.0
        inet6 addr: fe80::250:56ff:fe81:15/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:218643 errors:0 dropped:0 overruns:0 frame:0
        TX packets:8516 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:18348530 (17.4 MiB)  TX bytes:1933501 (1.8 MiB)
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:627 errors:0 dropped:0 overruns:0 frame:0
        TX packets:627 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:38076 (37.1 KiB)  TX bytes:38076 (37.1 KiB)
```

### 单一网卡配置第二个IP地址的方法（临时性）

在etht0上配置第二个IP地址，并假设第二个IP地址为192.168.233.228。此方法只能临时使用，在重新启动服务器或是重新启动网络服务后就会消失，如果每次重新启动时，都要使用此配置，就要增加网卡的配置文件。

```
[root@localhost /]#ifconfig eth0:0 192.168.233.228 up//添加第二个IP到eth0：0
[root@localhost /]#ip addr show                    //查看网卡IP地址信息
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:50:56:81:00:15 brd ff:ff:ff:ff:ff:ff
    inet 192.168.233.229/24 brd 192.168.233.255 scope global eth0
    inet 192.168.233.228/24 brd 192.168.233.255 scope global secondary eth0:0
    //第二个IP地址
    inet6 fe80::250:56ff:fe81:15/64 scope link
       valid_lft forever preferred_lft forever
3: sit0: <NOARP> mtu 1480 qdisc noop state DOWN
    link/sit 0.0.0.0 brd 0.0.0.0
```

**说明**

注意，此命令只可以配置固定IP地址，不可以使用DHCP服务自动获取方法，所以IP地址不可以空白。eth0:0代表第一块网卡的第二个IP名称，第一块网卡的第三个IP名称就为eth0:1，依此类推。

有增加就有删除，在执行删除命令时dev eth0是指实体网卡，不能输入eth0:0。最简单的方法就是重新启动网卡就会消失。

```
[root@localhost /]# ip addr delete 192.168.233.228 dev eth0 //删除第二个IP
Warning: Executing wildcard deletion to stay compatible with old scripts.
         Explicitly specify the prefix length (192.168.233.228/32) to avoid this warning.
         This special behaviour is likely to disappear in further releases,
         fix your scripts!
[root@localhost /]# ip addr show                    //再次查看网卡信息
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:50:56:81:00:15 brd ff:ff:ff:ff:ff:ff
    inet 192.168.233.229/24 brd 192.168.233.255 scope global eth0 //无eth0:0
    inet6 fe80::250:56ff:fe81:15/64 scope link
       valid_lft forever preferred_lft forever
3: sit0: <NOARP> mtu 1480 qdisc noop state DOWN
    link/sit 0.0.0.0 brd 0.0.0.0
```

# 单一网卡配置第二个IP地址的方法（固定）

先到网卡配置文件目录，创建第二个IP地址的网卡配置文件，将原来网卡的配置文件ifcfg-eth0复制成ifcfg-eth0:0，复制好第二个IP的网络配置文件后，编辑该配置文件，将配置文件中的DEVICE由eth0改成eth0:0，修改【IPADDR=192.168.233.228】，将BOOTPROTO改成static，剩下的配置信息与其他网络配置文件一样。

```
[root@localhost /]#cd /etc/sysconfig/network-scripts//进入网卡配置文件目录
[root@localhost network-scripts]# cp ifcfg-eth0  ifcfg-eth0:0
                                      //复制 ifcfg-eth0 至 ifcfg-eth0:0
[root@localhost network-scripts]# vi ifcfg-eth0:0
                                      //编辑第一块网卡的第二个 IP 地址
DEVICE=eth0:0            //网卡的名称为 eth0，第二个 IP 地址则要输入为 eth0:0
HWADDR=00:50:56:81:00:15
NM_CONTROLLED=yes
ONBOOT=yes
IPADDR=192.168.233.228           //修改成第二个 IP 地址
BOOTPROTO=static
NETMASK=255.255.255.0
TYPE=Ethernet
GATEWAY=192.168.233.254
DNS1=192.168.233.3
IPV6INIT=no
USERCTL=no
```

接下来就是重新启动网络服务或重新启动服务器，检查配置是否生效。

```
[root@localhost network-scripts]# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
```

重新启动后，再次检查配置有没有消失，如果没有表示配置成功。

```
[root@localhost network-scripts]# ip addr show     //检查网卡信息
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:50:56:81:00:15 brd ff:ff:ff:ff:ff:ff
    inet 192.168.233.229/24 brd 192.168.233.255 scope global eth0
    inet 192.168.233.228/24 brd 192.168.233.255 scope global secondary eth0:0
//第二个 IP 地址
    inet6 fe80::250:56ff:fe81:15/64 scope link
       valid_lft forever preferred_lft forever
3: sit0: <NOARP> mtu 1480 qdisc noop state DOWN
```

```
    link/sit 0.0.0.0 brd 0.0.0.0
```

再由另一台计算机测试网络连接是否畅通。

```
C:\Documents and Settings\user>ping 192.168.233.228
Pinging 192.168.233.228 with 32 bytes of data:
Reply from 192.168.233.228: bytes=32 time=12ms TTL=62
Reply from 192.168.233.228: bytes=32 time=1ms TTL=62
Reply from 192.168.233.228: bytes=32 time=1ms TTL=62
Reply from 192.168.233.228: bytes=32 time=1ms TTL=62
```

说明

删除第二个IP时将配置文件ifcfg-eth0:0也删除，然后重新启动操作系统。

## 2.4 双网卡带宽绑定

通常想要实现带宽绑定，主要是为了实现设备容错、负载均衡、端口绑定。一台服务器都会有两块网卡，不过一般只会使用一块网卡，此时将服务器做带宽绑定是有必要的，以免浪费另一块网卡，也可以减轻一块网卡工作的负担。

检查网络配置可以看到有两块网卡eth0和eth1，现在要将两块网卡带宽绑定，必须配置这两块网卡。

```
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:91:5F:2E
          inet addr:192.168.233.200  Bcast:192.168.233.255
          Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe91:5f2e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4745 (4.6 KiB)  TX bytes:5831 (5.6 KiB)

eth1      Link encap:Ethernet  HWaddr 00:0C:29:91:5F:38
          inet addr:192.168.233.201  Bcast:192.168.233.255
          Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe91:5f38/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:422 (422.0 b)  TX bytes:746 (746.0 b)
```

先进入network-scripts目录，编辑第一块网卡eth0的配置文件，内容如以下所示，编辑完后保存文档。

```
[root@localhost network-scripts]# cd /etc/sysconfig/network-scripts
```

```
[root@localhost network-scripts]# vi ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=none
USERCTL=no
MASTER=bond0      //带宽绑定后的网卡配置，bond0 为绑定带宽的网卡名称
SLAVE=yes
```

再来编辑第二块网卡eth1的配置文件，增加内容与eth0配置文件一样，编辑完后保存文档。

```
[root@localhost network-scripts]# vi ifcfg-eth1
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=none
USERCTL=no
MASTER=bond0     //带宽绑定后的网卡配置，bond0 为绑定带宽的网卡名称
SLAVE=yes
```

接下来创建一个新的配置文件ifcfg-bond0，内容如下，第5、6、7、8行请根据环境进行IP配置，编辑完后保存文档。

```
[root@localhost network-scripts]# vi ifcfg-bond0
DEVICE=bond0
ONBOOT=yes
IPADDR=192.168.233.200          //带宽绑定后的 IP 地址
BOOTPROTO=none
NETMASK=255.255.255.0
GATEWAY=192.168.233.1
DNS1=192.168.233.1
```

编辑modprobe.conf，增加两行配置信息，miimon=100为每100毫秒（0.1秒）检查网络一次，可根据个人需求进行设置，这代表网络如果断线，0.1秒就会恢复连接，mode为网卡工作模式，共有7种，通常设置0、1、6这几种。

```
[root@localhost /]# vi /etc/modprobe.conf
alias bond0 bonding
options bond0 miimon=100 mode=1
```

Mode模式的功能如下表所示。

| mode | 功能 | 功能说明 |
|---|---|---|
| 0 | balance-rr | 负载均衡模式需有 switch 配置（trunk）支持才能发挥实际效果，具有容错功能，其中一块网卡失效仍可持续工作 |
| 1 | active-backup | 同一时间只有一块网卡工作，Active Slave 其中一块网卡断线时自动启用另一块网卡，不需 switch 支持 |
| 2 | balance-xor | 具容错作用 |
| 3 | broadcast | 所有网卡一起收发网络数据包，具容错功能，其中一块网络卡断线仍可持续工作 |

（续表）

| mode | 功能 | 功能说明 |
| --- | --- | --- |
| 4 | 802.3ad | 无实际功能，不建议使用 |
| 5 | balance-tlb | 发送数据包自动负载均衡，接收数据包由 Current Active Slave 负责，具容错功能，其中一块网络卡失效仍可持续工作，不需 switch 支持及配置 |
| 6 | balance-alb | 发送及接收皆自动负载均衡，具容错功能，其中一块网络卡断线时仍可持续工作，网络卡区动程序需支持 setting hardware address 功能，不需 switch 支持及配置 |

全部配置完成后，重新启动网卡，让bond0重新启动。

```
[root@localhost /]# service network restart
Shutting down interface bond0:                              [  OK  ]
Shutting down loopback interface:                           [  OK  ]
Bringing up loopback interface:                             [  OK  ]
Bringing up interface bond0:                                [  OK  ]
```

查看网卡配置信息，可以看到只有bond0有配置IP地址，不过其他两块网卡仍正常工作。

```
[root@localhost /]# ifconfig
bond0     Link encap:Ethernet  HWaddr 00:0C:29:91:5F:2E
          inet addr:192.168.233.200  Bcast:192.168.233.255
          Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe91:5f2e/64 Scope:Link
          UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:3491 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1699 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:330865 (323.1 KiB)  TX bytes:268485 (262.1 KiB)

eth0      Link encap:Ethernet  HWaddr 00:0C:29:91:5F:2E
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:2670 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1669 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:245559 (239.8 KiB)  TX bytes:265153 (258.9 KiB)

eth1      Link encap:Ethernet  HWaddr 00:0C:29:91:5F:2E
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:821 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:85306 (83.3 KiB)  TX bytes:3566 (3.4 KiB)
```

查看bonding状态，可以看到bond0的配置信息，这样就是带宽绑定成功。

```
[root@localhost /]# cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v3.5.0 (November 4, 2008)
```

```
Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
Currently Active Slave: eth0
MII Status: up
MII Polling Interval (ms) : 100
Up Delay (ms) : 0
Down Delay (ms) : 0

Slave Interface: eth0
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:0c:29:91:5f:2e

Slave Interface: eth1
MII Status: up
Link Failure Count: 0
Permanent HW addr: 00:0c:29:91:5f:38
```

## 2.5 禁用 IPv6支持提高网络效率

IPv6协议是下一代 IP地址的通信协议，目前所使用的IPv4协议，因IP地址随互联网用户的快速增长，很快就会面临用完的困境，所以IPv6协议势必成为未来的趋势。而绝大多数的Linux操作系统都支持IPv6协议，甚至很多主流的Linux操作系统默认安装后可直接启用。可以根据实际应用禁用IPv6支持。检查网络配置，如果有inet6 addr相关信息，表示IPv6协议是开启状态。

```
[root@localhost ~]# ifconfig
eth0  Link encap:Ethernet  HWaddr 00:50:56:81:00:29
      inet addr:192.168.233.232  Bcast:192.168.233.255  Mask:255.255.255.0
      inet6 addr: fe80::250:56ff:fe81:29/64 Scope:Link //IPv6 协议开启状态
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:4102784 errors:0 dropped:0 overruns:0 frame:0
      TX packets:37805 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:295272673 (281.5 MiB)  TX bytes:4274203 (4.0 MiB)
```

禁用IPv6支持的方法很简单，即在disable-ipv6.conf配置文件中增加install ipv6 /bin/true，然后重新启动，配置才会生效。

```
[root@localhost ~]# echo "install ipv6 /bin/true" > /etc/modprobe.d/disable-ipv6.conf
```

重新启动网络服务后，再次检查网卡信息，则不会再出现inet6 addr，代表IPv6已停用。

```
[root@localhost ~]# ifconfig
eth0  Link encap:Ethernet  HWaddr 00:50:56:81:00:29
      inet addr:192.168.233.232  Bcast:192.168.233.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
      RX packets:82 errors:0 dropped:0 overruns:0 frame:0
      TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:7598（7.4 KiB） TX bytes:5582（5.4 KiB）
```

有关闭就有开启，不然要使用IPV6时，却不知如何开启就麻烦了。要启用IPv6协议，只要删除配置文件中的install ipv6 /bin/true或删除disable-ipv6.conf文件即可。

```
[root@localhost ~]# vi /etc/modprobe.d/disable-ipv6.conf
install ipv6 /bin/true            //删除此行
```

# 第3章

# 远程管理工具

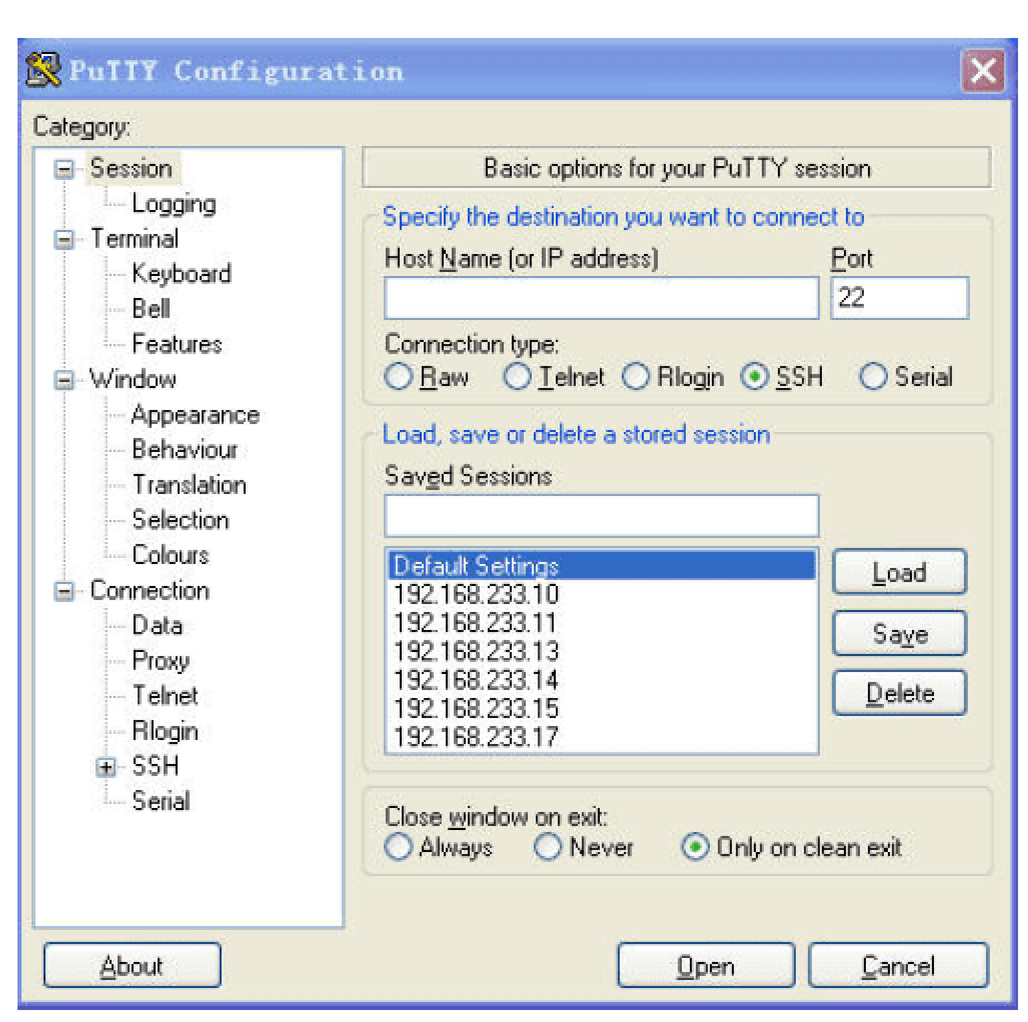
## 3.1 PuTTY远程连接工具

PuTTY官方网站：http://www.chiark.greenend.org.uk/~sgtatham/putty/。

PuTTY是一种加密的Telnet/SSH 安全远程连接工具，历史悠久。它是远程连接Linux系统很棒的工具，不过此工具有一个缺点，在非英文语系的系统中，会出现乱码。

### PuTTY登录方式

在【Host Name】中输入IP地址，SSH端口默认为22，输入完毕后，按【Open】即可连接，如果想保留主机的IP地址，即可在【Saved Sessions】中输入该地址，按【Save】保存。




输入账号和密码后，即可进入CentOS操作系统。

```
root@localhost:~
login as: root
root@192.168.233.230's password:
Last login: Sun Aug 26 20:56:44 2012 from 192.168.233.1
[root@localhost ~]#
```

## 3.2 PieTTY远程连接工具

PieTTY官方网站：http://www.csie.ntu.edu.tw/~piaip/pietty/。

PuTTY 是一个小巧方便的 Telnet/SSH 安全远程连接工具，对于初学者来说它的使用界面过于复杂，而且在用于非英语语言时有非常多的问题。PieTTY 源自于 PuTTY，在使用界面上有大幅度改进，对初学者来说是易学易用的工具。目前暂时没有简体中文版本。

PieTTY 0.4 系列是修改自 PuTTY 0.57/0.58 的版本，以稳定与修正为主。 主要的特色有:

- 简单易用的界面。主要的功能都可以从选项中选择。
- 完全兼容于传统 PuTTY 工具，之前的配置全部可直接使用。
- 更强的连接整合管理（session management），自动保存配置。
- 高度自定义（customizable）窗口显示效果。
- 半透明显示（多种显示引擎以配合各种硬件设备与窗口立体阴影，配合无框显示模式效果奇佳）。
- 支持ssh://方式的连接，可整合系统设置为ssh://与telnet://处理工具。
- 对于各种网址 URL 可直接单击打开，还有多种可选用的视觉效果。
- 支持拖曳文件（Drag-n-drop）即可进行SCP 上传。

对于非英文字符，PieTTY 特别增强的部分有:

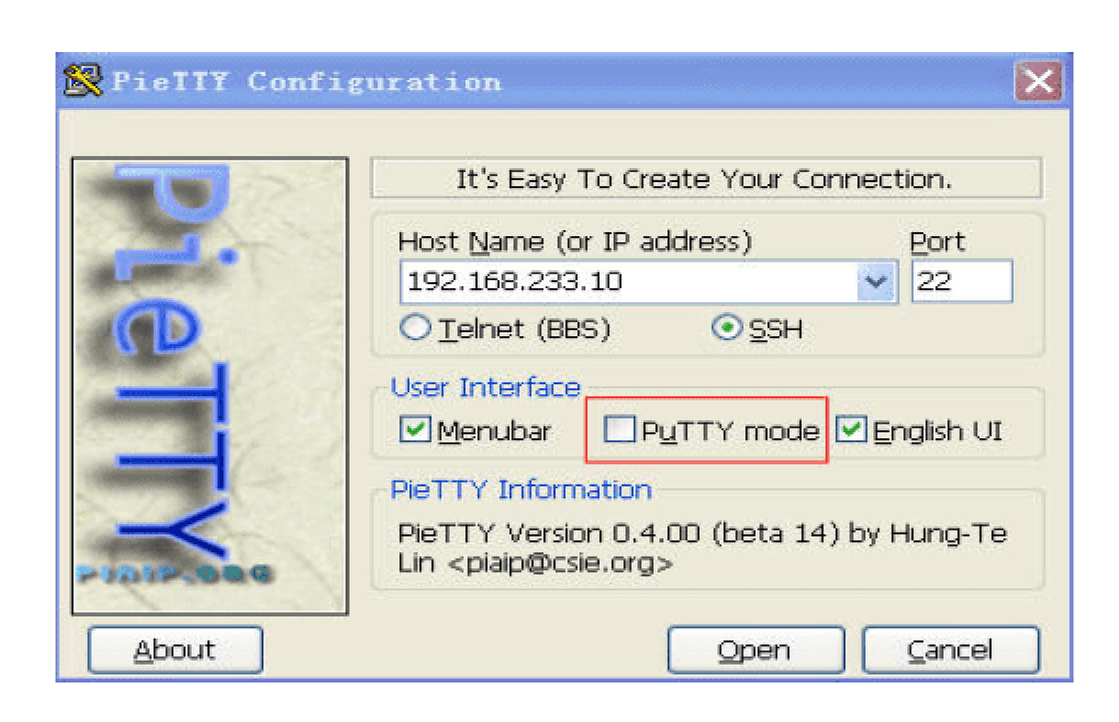
- 可使用英文等其他字符集，而且不用配置字符集（CHARSET）(传统 PuTTY 则一定要配置正确才行)。
- 在非 UTF8 模式下 PieTTY 的光标也能正确显示（传统 PuTTY 会破坏光标上的多位字符串）。
- 重复使用时屏幕完全不闪动（PuTTY 在非 UTF8 字符集中会闪）。

对繁体中文及 BBS 环境有更多的增强功能:

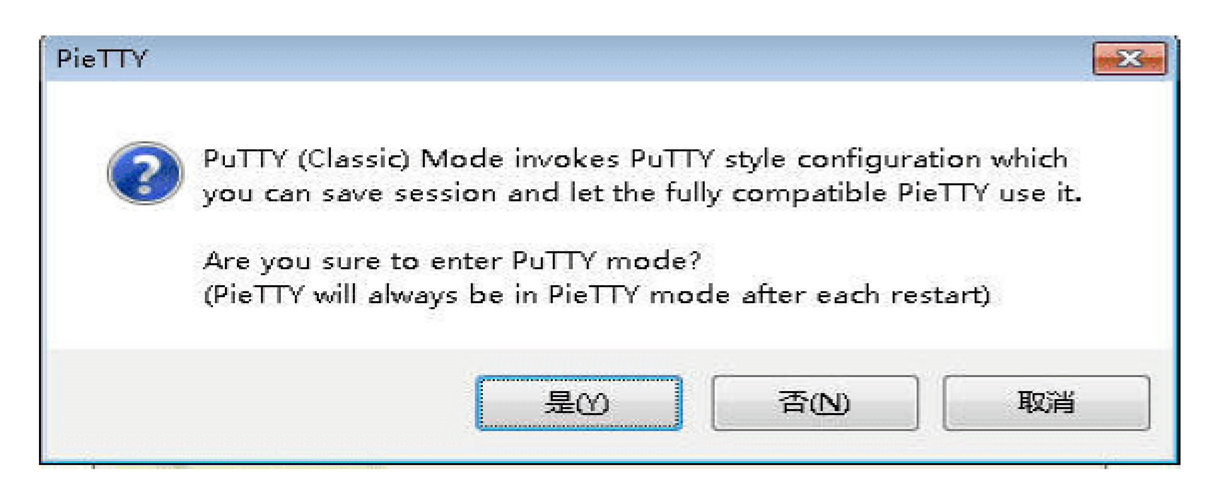
- 内置 Big5-2003 + 相容Unicode补完计划2.40版字码表，不安装 Unicode 补完即可正常剪贴或输入日文等。
- 内置简单的汉字（简繁）转换，方便阅读。

- 支持一字双色的ANSI码。
- 复制文字时可自动将属性颜色以 ANSI 码或 IRC 形式加入，BBS 与 IRC 互贴彩色不是梦！

启用PieTTY工具后输入主机名或IP地址，端口Port默认为22，按下【Open】即可以连接，使用模式如果选择【PuTTY mode】的话，选项会与PuTTY一样。




第一次启动时会提示是否要进入PuTTY兼容模式，按【是】进入系统。




启动后的界面与PuTTY相似，不过工具栏上多出了一些功能选项，可以配置字符等功能。

```
root@localhost:~ [80x24]
Connection  Edit  View  Transfer  Option  Help
login as: root
root@192.168.233.230's password: *******
Last login: Sun Aug 26 21:16:50 2012 from 192.168.233.1
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
```

## 3.3 WinSCP文件传输工具

官方网站：http://winscp.net/eng/docs/lang:cht。

WinSCP 是在Windows中使用SSH的开源图形化SFTP客户端，同时支持SCP协议。它的主要功能就是在本地与远程计算机间安全地复制文件。

## 下载WinSCP工具

下载地址：http://winscp.net/eng/download.php。

下载版本有两种，Installation package安装版和Portable executables免安装版。现在的版本已经支持多国语言，为了能正常支持简体中文，需要使用Installation package版本安装，然后下载简体中文（Simplified Chinese）插件，将插件包解压缩到 WinSCP 安装目录即可。但是免安装版本无法使用简体中文。

## WinSCP介绍

- 图形用户界面。
- 多国语言界面。
- Windows整合（拖放文件、URL、快捷方式）。
- 支持所有常用文件操作。
- 支持基于 SSH-1 和 SSH-2 上的SFTP 与 SCP 协议。
- 支持批处理脚本和命令行模式。
- 多种半自动、自动的目录同步方式。
- 内置文本编辑器。
- 支持 SSH 密码、键盘互动、公钥与 Kerberos（GSS）认证方式。
- 内置 Pageant（PuTTY Agent）完整支持公钥认证法。
- 提供 Windows Explorer 与 Norton Commander 界面。
- 可选择保存会话信息。
- 可将设置保存在配置文件中而非注册表中，适合在移动介质上操作。

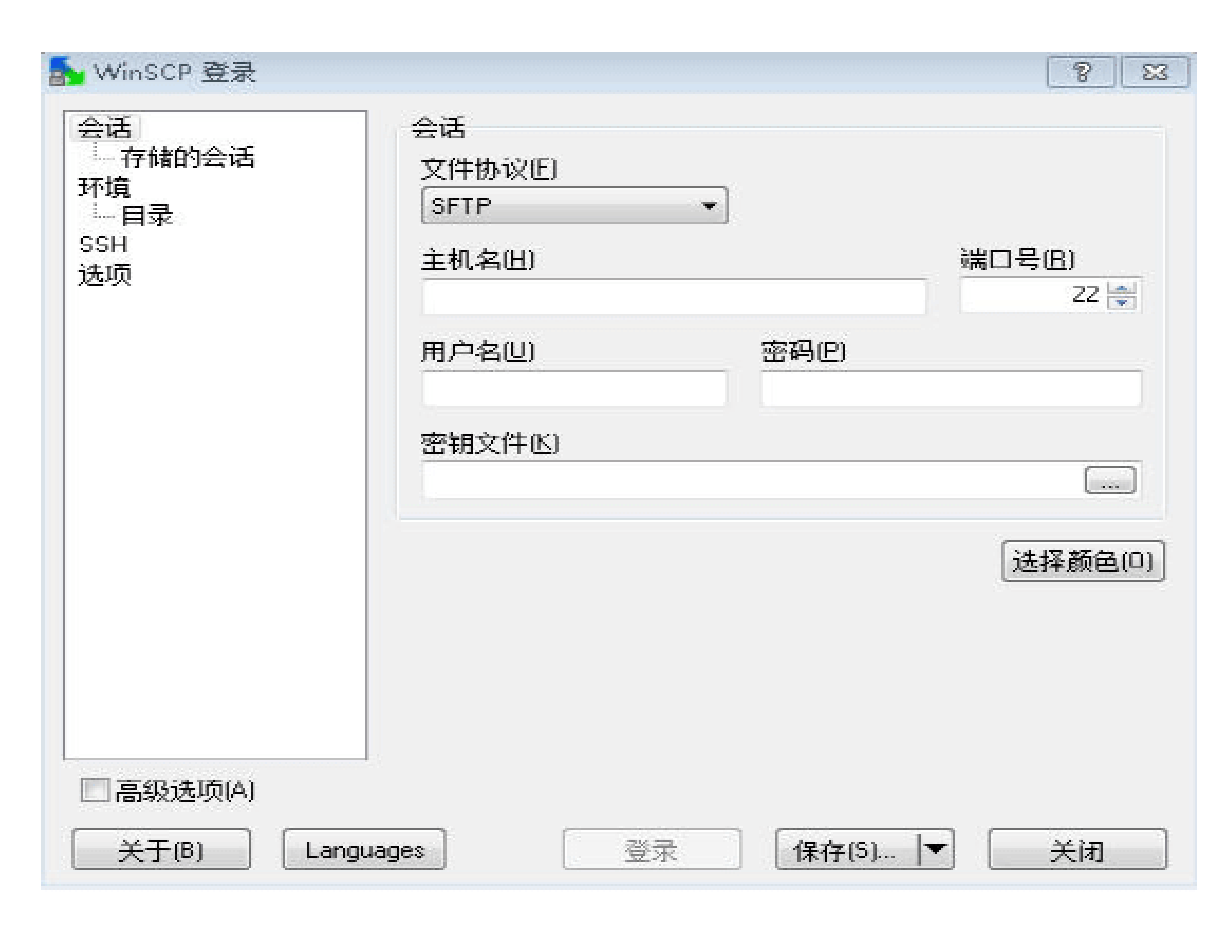
WinSCP可以进行所有基本的文件操作，包括下载与上传文件，同时允许为文件和目录重新命名、新增文件夹、修改内容、建立符号链接（symbolic links）与快捷方式。

连接远程主机：WinSCP可以连接一台提供SSH（Secure Shell）服务与SFTP（SSH File Transfer Protocol）或SCP（Secure Copy Protocol）服务的主机，这些服务通常是UNIX机器上的服务。SFTP是SSH-2协议标准的一部份，而SCP是SSH-1协议的标准。两种协议都可以在SSH版本上运行。WinSCP同时支持SSH-1与SSH-2。

工具操作界面：WinSCP有两种可以选择的操作界面与许多配置选项，两种可选界面允许用户管理远程或本地的文件。在安装时可以选择用户所喜欢的操作界面，也可以在选项中改变它。如果是第一次使用WinSCP，可能会希望选择比较熟悉的文件操作界面，或是已习惯被应用在许多文件管理工具中（如Total Commander、FAR、Altap Salamander）的Norton Commander概念的双窗界面，可选择这个操作界面。双窗界面的设计可以简单地使用键盘操作工具，甚至不用碰触鼠标，使用此界面可以更快地操作WinSCP工具。

## WinSCP操作使用

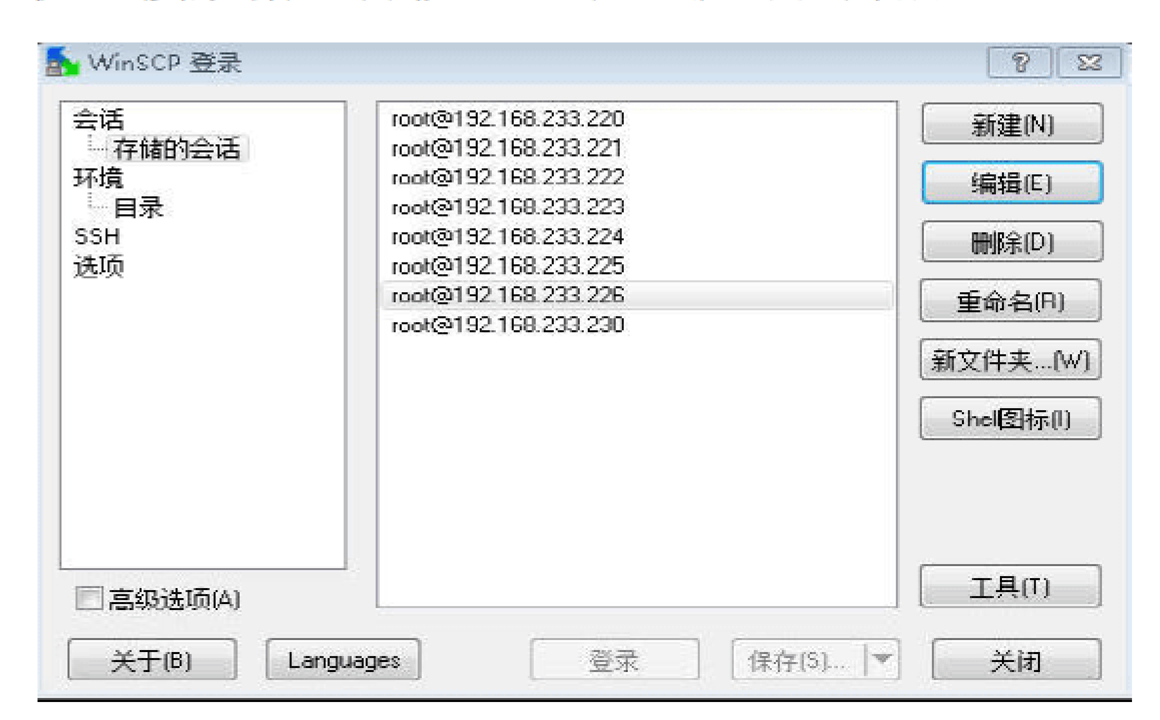
执行WinSCP程序打开操作界面，在【会话】选项中，可以输入主机名或IP地址、用户名、密码，如果有密钥文件也可以导入，输入登录服务器信息后按下【登录】即可开启WinSCP工具，如果想保存登录主机的信息，即可按下【保存】，这样就不用每次登录的时候输入主机信息了。



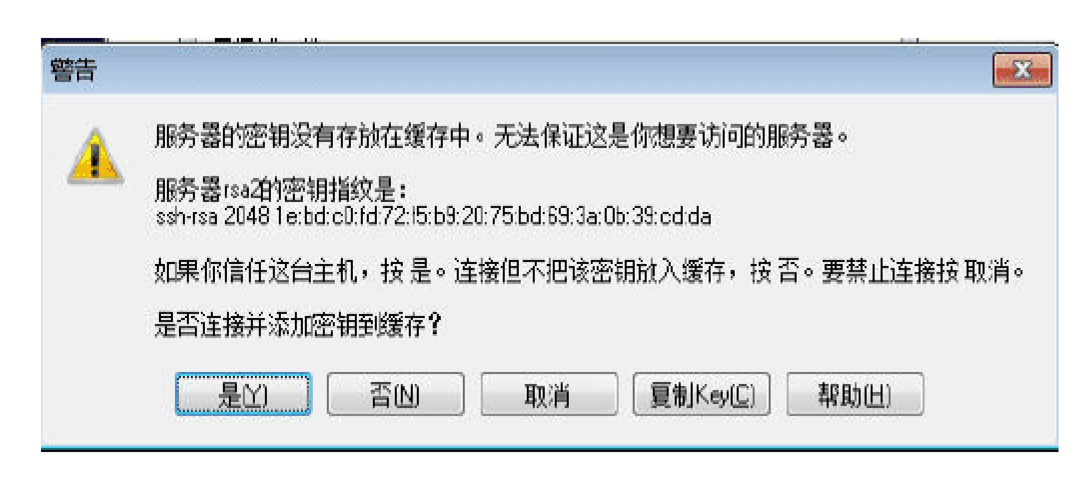

按【确定】，WinSCP会将连接服务器信息保存，也会询问要不要保存密码，如果没勾选【保存密码】，则不会保存密码信息。



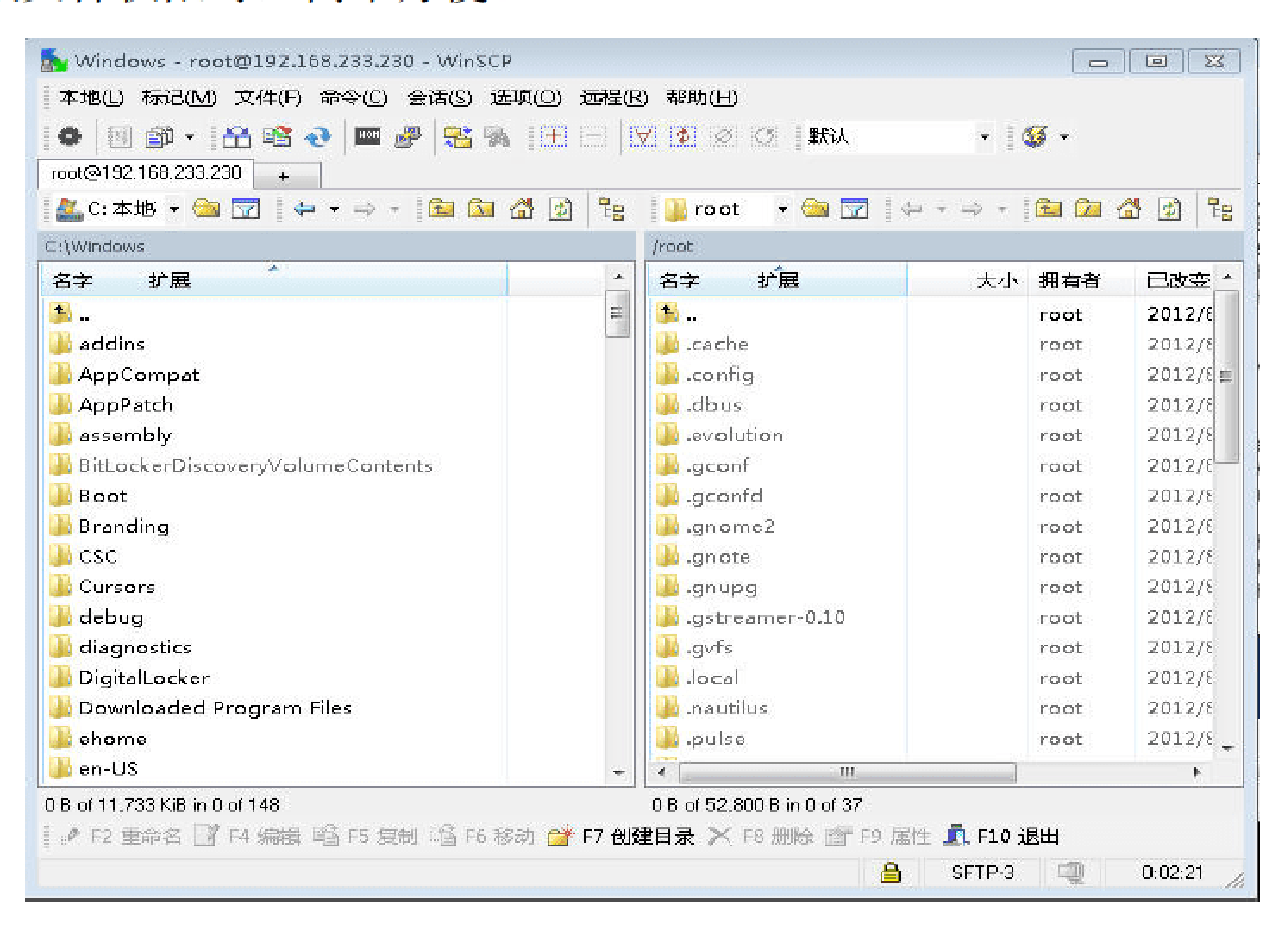

保存连接服务器数据后，会回到WinSCP登录界面，以后只要在【会话】下面的【存储的会话】中选择保存的主机连接数据，再按【登录】就可以开启WinSCP了。




第一次登录主机都会出现警告信息，警告没有连接服务器的密钥信息的缓存信息，是否要将密钥信息保存到缓存中，按【是】即保存密钥信息，也可以登录服务器。




WinSCP登录界面如下图所示，其操作方式和Windows的文件操作一样，可以重命名、复制、修改、更改文件权限等，简单方便。




## 3.4 Webmin系统管理工具

Webmin官方网站：http://www.webmin.com/。

Webmin 体验网站：http://webmin-demo.virtualmin.com/。

Webmin允许管理员通过浏览器访问CentOS操作系统的各种管理功能并完成相应的管理工作。官方网站还提供体验网站，登录账号和密码都为Demo，若未使用过此工具，可以先登录体验一下。

### 下载Webmin软件并安装

Webmin安装方法很简单，以往是使用tar/gzip安装，现在提供RPM方式，这为安装人员带来许多便利，可利用wget命令直接下载到CentOS服务器安装。

```
[root@localhost /]# wget
http://prdownloads.sourceforge.net/webadmin/webmin-1.590-1.noarch.rpm
```

下载Webmin软件完成后就可以进行安装了，不过安装前，先确认是否安装Apache，Webmin是工作在Apache网站服务器上的，确认安装Apache网站软件后，立即进行Webmin软件的安装。

```
[root@localhost /]# rpm -ivh webmin-1.590-1.noarch.rpm   //安装 Webmin 软件
warning: webmin-1.590-1.noarch.rpm: Header V3 DSA/SHA1 Signature, key ID 11f63c51: NOKEY
Preparing...                ########################################### [100%]
Operating system is CentOS Linux
   1:webmin                 ########################################### [100%]
Webmin install complete. You can now login to http://localhost.localdomain:10000/
as root with your root password.
```

## 配置防火墙

Webmin默认使用的端口为10000，需要编辑防火墙配置文件开放该端口。

```
[root@localhost /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p tcp --dport 10000 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

修改防火墙配置文件后，必须重新启动防火墙程序，配置信息才会生效。

```
[root@localhost]# service iptables restart
iptables: Flushing firewall rules:                        [  OK  ]
iptables: Setting chains to policy ACCEPT: filter         [  OK  ]
iptables: Unloading modules:                              [  OK  ]
iptables: Applying firewall rules:                        [  OK  ]
```

## 重新启动Apache服务

防火墙配置完成后，重新启动Apache服务，Webmin才可以正常使用。

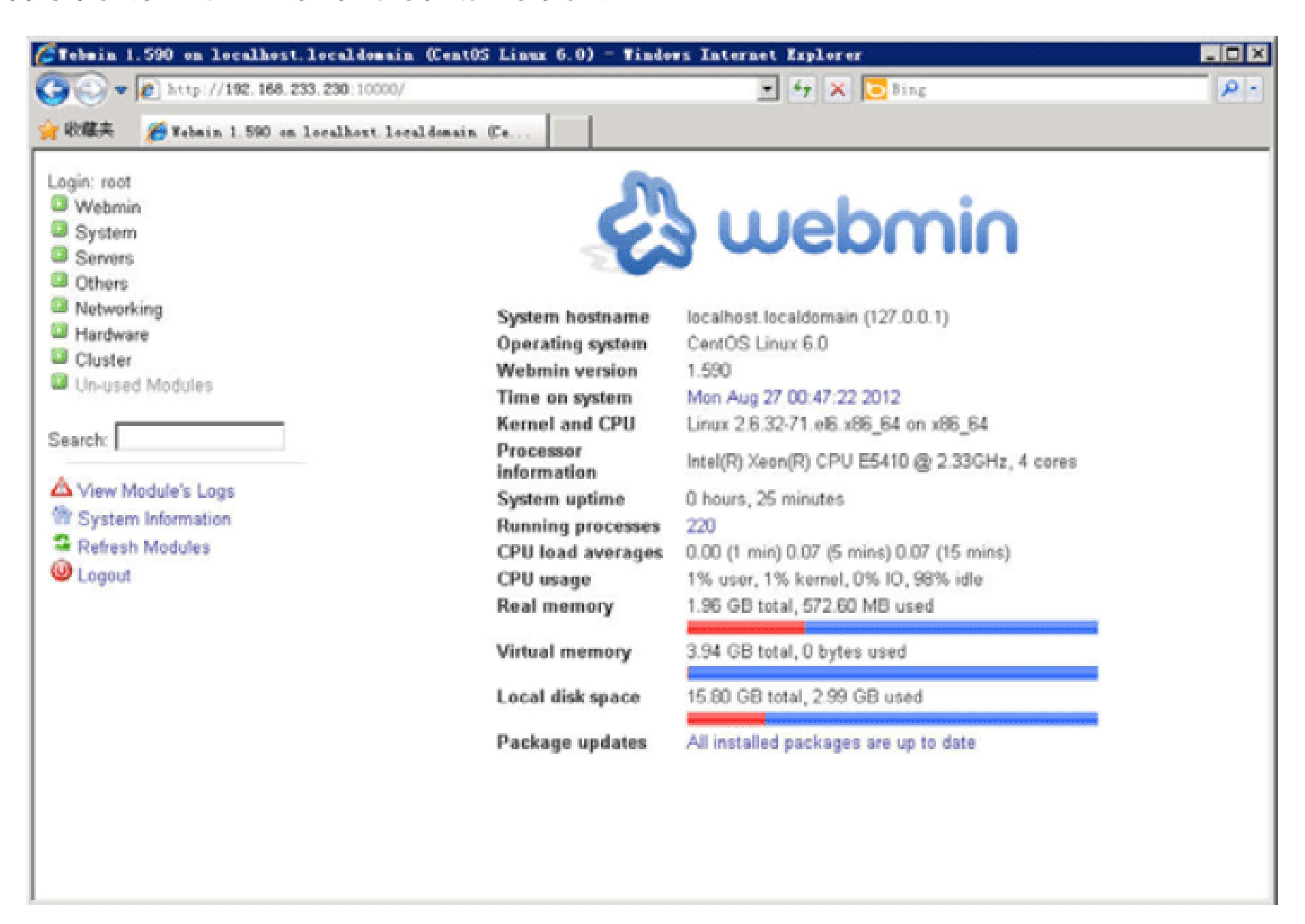
```
[root@localhost]# service httpd restart
Stopping httpd:                                             [  OK  ]
Starting httpd:                                             [  OK  ]
```

## 使用Webmin工具

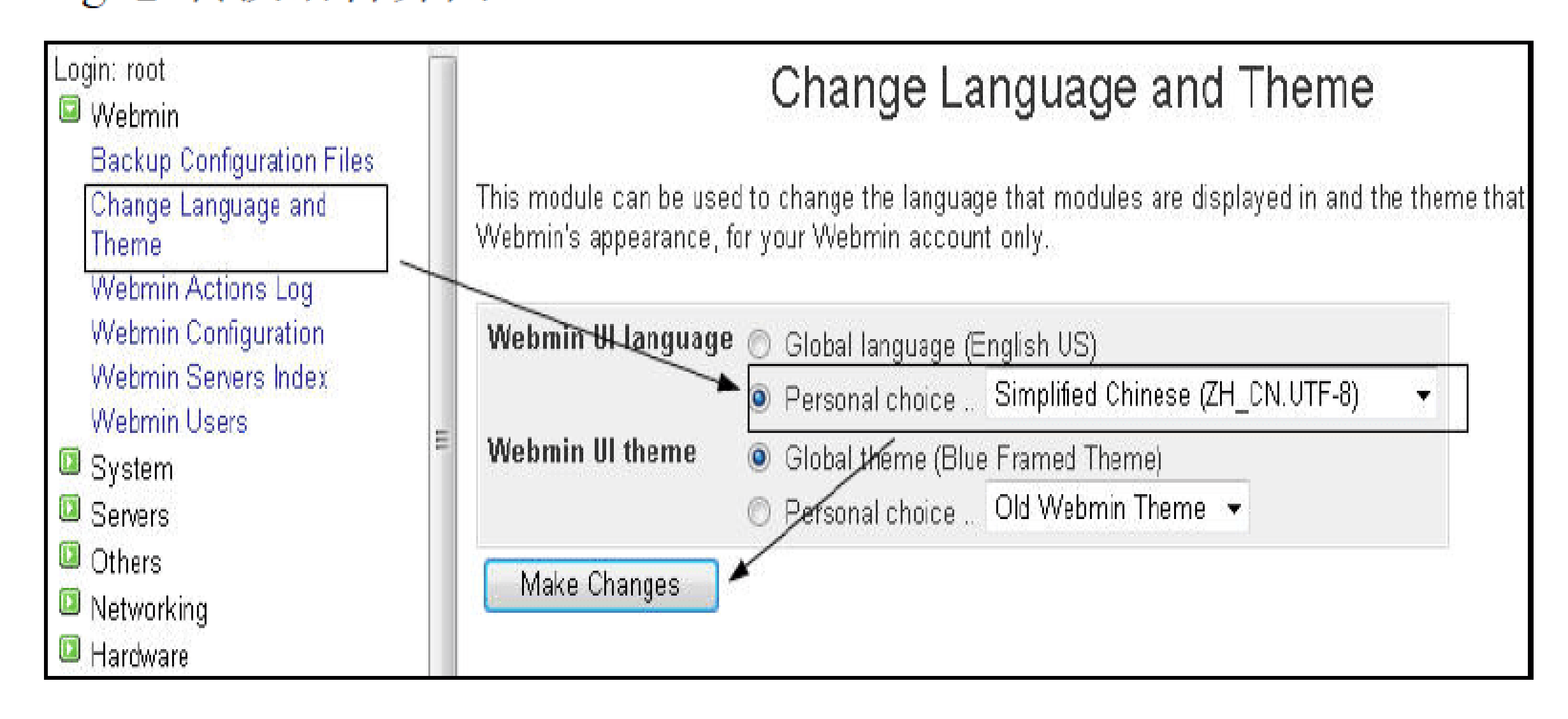
一切安装配置完成后，打开浏览器，输入【http://IP地址:10000】，Webmin会出现输入账号和密码的界面，账号和密码为系统管理者账号，默认使用root账号登录。

Login to Webmin
You must enter a username and password to login to the Webmin server on 192.168.233.230.
Username
Password
Remember login permanently?
Login Clear

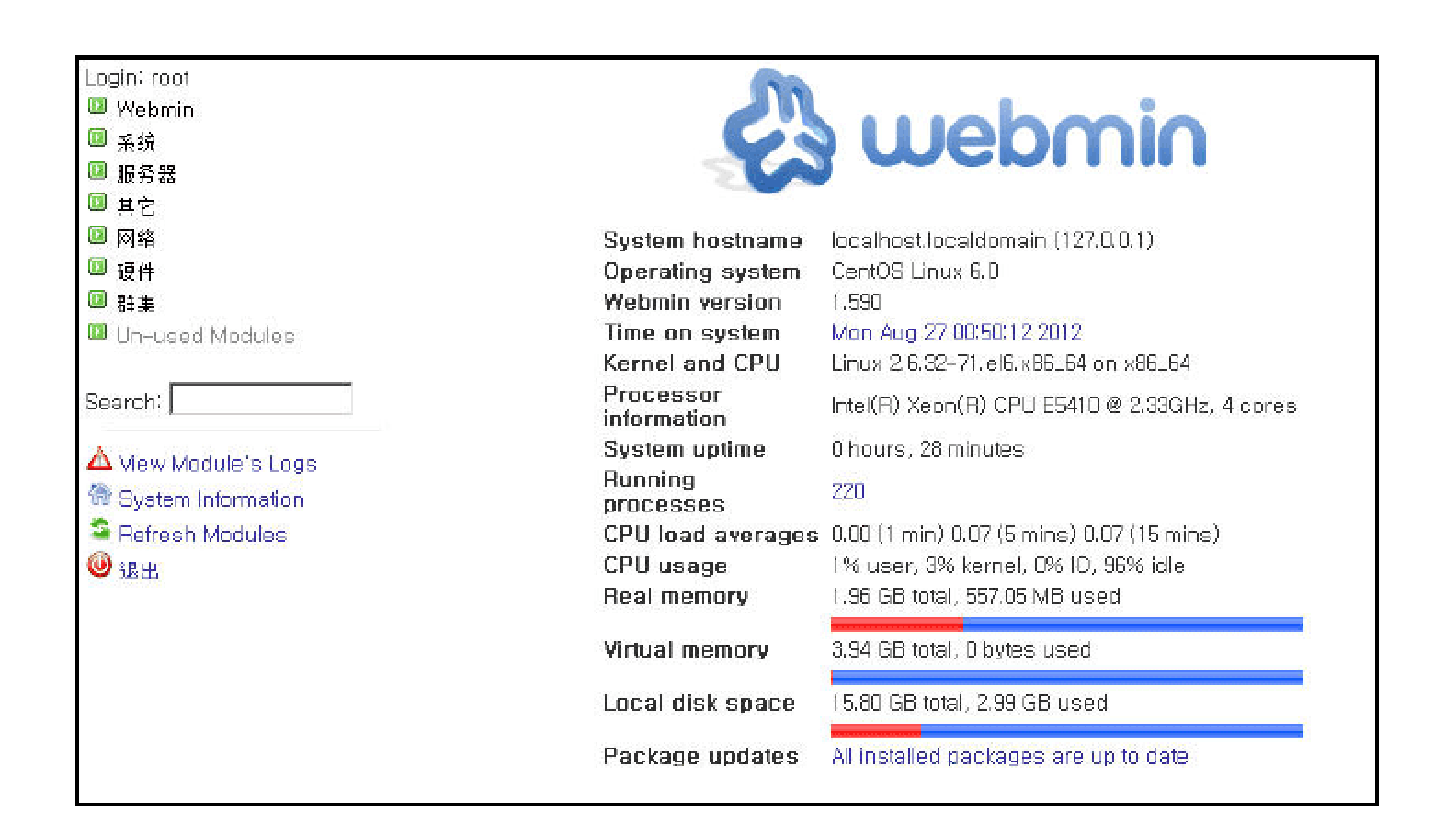
Webmin操作界面如下，默认为英文界面。




如果不习惯默认英文界面，可以自行修改，在【Webmin】→【Change Language and Theme】→【Webmin UI Language】→【Personal choice】中，选择Simplified Chinese（ZH_CN.UTF-8），按【Make Change】转换语言界面。




将浏览器关闭并重新开启后，默认语言就为简体中文。对于如何使用Webmin，在此不用多说，界面很容易上手。




## 使用yum方法安装

默认使用yum时无法安装Webmin，原因是该软件没有在官方站点存放，也没有放进系统安装光盘。虽然以前要用tar方式安装，但是之后编译出了RPM安装包，所以只好自行配置更新站点。在/etc/yum.repo.d中创建webmin.repo文件，编辑完成后保存退出，然后导入Webmin开放源代码的GPG的数字签名。

```
[root@localhost /]# vi /etc/yum.repos.d/webmin.repo
[Webmin]
name=Webmin Distribution Neutral
baseurl=http://download.webmin.com/download/yum    //配置 webmin 安装来源站点
enabled=1
[root@localhost /]# rpm --import http://www.webmin.com/jcameron-key.asc
```

然后使用yum方式进行安装，这次就会出现Webmin安装软件信息，其他相关配置和之前的配置相同。

```
[root@localhost /]# yum install webmin
Dependencies Resolved

========================================================================
 Package       Arch          Version            Repository        Size
========================================================================
Installing:
webmin         noarch         1.590-1             Webmin          16 M

Transaction Summary
========================================================================
Install        1 Package (s)
Upgrade        0 Package (s)

Total download size: 16 M
```

# 第 4 章

# 系统管理技巧

## 4.1 登录前后显示信息

登录前显示的信息除了是一句标语，也可以达到提醒的效果，类似备忘录的功能，下面介绍登录前后如何配置显示信息。

CentOS 6.x操作系统登录前的信息，默认只有操作系统版本号及内核版本号，接下来就是输入账号。

```
CentOS Linux release 6.0 (Final)
Kernel 3.6.32-71.el6.x86_64 on x86_64
Localhost login:
```

如果需要显示信息，需编辑/etc/issue配置文件，在最后加上Welcome，保存后退出。

```
[root@localhost /]# vi /etc/issue
CentOS Linux release 6.0 (Final)
Kernel \r on an \m
Welcome      //登录前显示的文字信息
```

若要测试刚才配置是否会生效，需要重新登录，输入账号和密码前就会有登录前配置的信息，如果出现配置的信息，表示配置成功。

```
CentOS Linux release 6.0 (Final)
Kernel 3.6.32-71.el6.x86_64 on x86_64
Welcome
Localhost login:
```

> **说明**
>
> 登录前显示的信息只能在本机登录时出现，使用PuTTY工具时不会看到此信息。

对于登录后显示的信息，需要编辑/etc/motd，输入所要显示的欢迎信息，保存后退出。

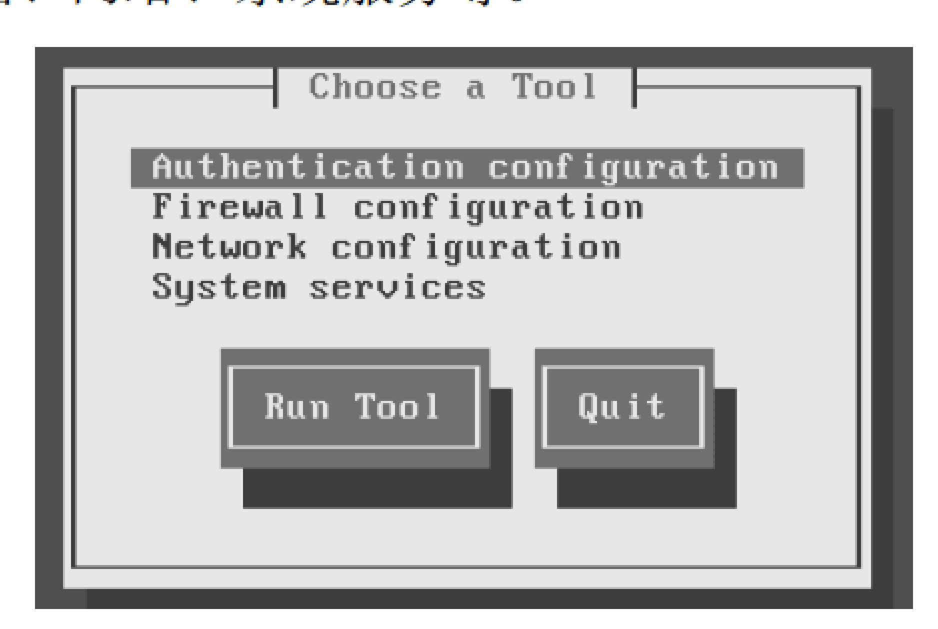
```
[root@localhost ~]# vi /etc/motd
check system          //登录后显示的文字信息
```

测试登录后是否会显示文字信息，如果出现所配置的信息，表示配置成功。

```
login as: root
root@192.168.233.229's password: *********
Last login: Wed Aug 24 19:19:02 2011 from 192.168.233.1
check system
```

## 4.2 配置Choose a Tool工具

CentOS 6.x操作系统内有一个很好用的工具，那就是输入【setup】命令就会出现Choose a Tool工具，可以配置防火墙、网络、系统服务等。




CentOS 6.x操作系统如果是最小化安装就无法使用该工具，因为最小化安装几乎什么软件都不装，所以要使用该工具都要自行安装。

```
[root@localhost ~]# setup
-bash: setup: command not found
```

虽然Choose a Tool工具对高级使用者没有影响，但是初学者还是很需要的，只要管理工具使用方便，不用管管理工具是高级还是低级，安装Choose a Tool工具需要以下相关软件，可以使用yum在线安装方法安装以下软件setuptool、ntsysv、system-config-firewall-tui、system-config-network-tui。

```
[root@localhost ~]# yum  install setuptool ntsysv system-config-firewall-tui
system-config-network-tui

Dependencies Resolved

=====================================================================
 Package                     Arch        Version             Repository   Size
=====================================================================
Installing:
 ntsysv                      x86_64      1.3.47-1.el6          base      28 k
```

```
 setuptool                    x86_64     1.19.9-3.el6         base  59 k
 system-config-firewall-tui  noarch     1.2.27-3.el6_0.2     updates  37 k
 system-config-network-tui   noarch     1.6.0.el6.2-1.el6    base 1.2 M
Installing for dependencies:
 crda                    x86_64     1.1.1_2009.11.25-3.el6   base   23 k
 dbus-python             x86_64     0.83.0-6.1.el6           base  204 k
 iw                      x86_64     0.9.17-4.el6             base   35 k
 libnl                   x86_64     1.1-12.el6_0.1           updates 120 k
 pciutils                x86_64     3.1.4-9.el6              base   82 k
 python-ethtool          x86_64     0.3-5.1.el6              base   21 k
 python-iwlib            x86_64     0.1-1.2.el6              base   14 k
 usermode                x86_64     1.102-3.el6              base  187 k
 wireless-tools          x86_64     1:29-5.1.1.el6           base   94 k
Updating for dependencies:
 system-config-firewall-base   noarch    1.2.27-3.el6_0.2    updates  418 k

Transaction Summary
===========================================================
Install      13 Package(s)
Upgrade       1 Package(s)

Total download size: 2.5 M
```

成功安装Choose a Tool工具后，再次输入【setup】检查是否可以使用，记住如果使用PuTTY就有可能不能正常显示，那是系统编码问题，所以建议在本机测试。

## 4.3 自动调整错误路径

通常输入路径时，会打错一两个字，就会出现错误信息，CentOS提供了一个小技巧，不过这个技巧不是万能的，只限于一两个字母路径打错，系统就会自动调整，其实系统也是根据输入的路径与相应的目录比对，然后修正，例如，要到etc目录却打成ect，就会出现找不到目录的情况。

```
[root@localhost ~]# cd /ect
-bash: cd: /ect: No such file or directory
```

### 修改.bashrc配置文件

在用户目录下修改.bashrc配置文件，在最后一行添加shopt -s cdspell，修改完后保存退出，此配置必须重新登录才会生效。

```
 [root@localhost ]# vi  ~/.bashrc
# .bashrc

# User specific aliases and functions

```

```
alias rm='rm -i'
alias cp='cp -i'
alias mv='mv -i'

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi
shopt -s cdspell        //在最后一行添加
```

> 说明
>
> 如果要其他用户也有这样的功能，则必须编辑/etc/bashrc，输入【vi /etc/bashrc】。

## 测试

要进入etc目录，故意输入成ect，检查系统是否会自动调整为etc。

```
[root@localhost ~]# cd /ect
/etc
[root@localhost etc]#
```

> 说明
>
> 如果输入错误字符过多，系统是无法修正的。

# 4.4 设置开机等待时间

CentOS 6.x操作系统每次开机时，都会有系统等待时间，此选项最常用到的地方就是修改密码，如果不需要修改密码的话，通常希望快速进入系统。为了快速进入操作系统，可以修改系统等待时间。

```
Press any key to enter the menu

Booting CentOS (2.6.32-71.el6.x86_64) in 2 seconds...
```

开机等待时间默认为5秒，将之设为0秒，保存后重新启动服务器，就会迅速跳过开机选项进入系统，不过建议设为1秒，这样忘记密码时，可以及时按下重新设置密码的选项。

```
[root@localhost /]# vi /boot/grub/menu.lst
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
```

```
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/mapper/VolGroup-lv_root
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5                                     //设置开机选项秒数，默认为 5 秒。
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.32-71.el6.x86_64)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-71.el6.x86_64 ro root=/dev/mapper/VolGroup-lv_root
rd_LVM_LV=VolGroup/lv_root rd_LVM_LV=VolGroup/lv_swap rd_NO_LUKS rd_NO_MD rd_NO_DM
LANG=en_US.UTF-8 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=pc KEYTABLE=us crashkernel=auto
rhgb quiet
        initrd /initramfs-2.6.32-71.el6.x86_64.img
```

## 4.5 自动注销登录账户

系统使用完后，正确的习惯是要退出或锁定，Windows及Linux操作系统都是如此，Windows是锁定账号，Linux必须输入命令才会退出，不过这个操作很多使用者都会忘记，所以必须设置系统空闲时间过长，就会自动退出。

编辑/etc/profile，设置系统在空闲时间超过30秒后，自动退出，保存设置后，此设置在下一次登录时才会生效，无需重新启动。

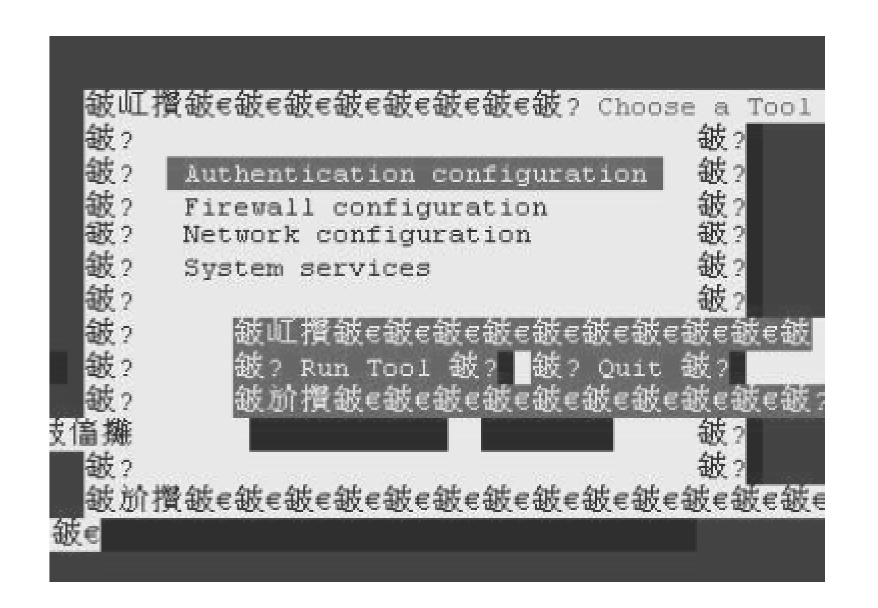
```
[root@localhost /]# vi /etc/profile
export TMOUT=30          //在最后一行添加，默认没有此行
```

> **说明**
>
> 单位为秒，注意字母有大小写之分，输入错误就不会生效。此功能支持远程连接工具，有些远程连接工具版本也会使用此设置，所以也会自动退出。

## 4.6 解决（Choose a Tool）工具界面乱码

文本模式设置工具（Choose a Tool）是一个方便的设置工具，虽然功能有限，但是常用的工具一样都不少，如Firewall、Network及System services等，不过使用PuTTY连接工具输入setup进入时，界面会出现乱码，本机使用不会有这种情况，此环境默认语言为英文。

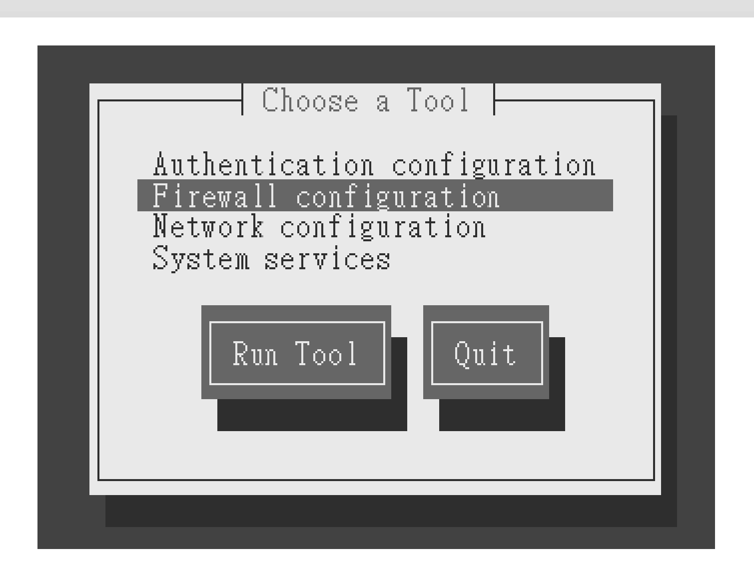
其实这种问题有几种解决方式，但是都不能完全解决问题，可根据需求情况进行不同的设置。




## 方法一

在PuTTY下输入【LANG=us】或【LANG=cn】，但重新开启PuTTY就要输入一次。

```
[root@localhost /]# LANG=us
```

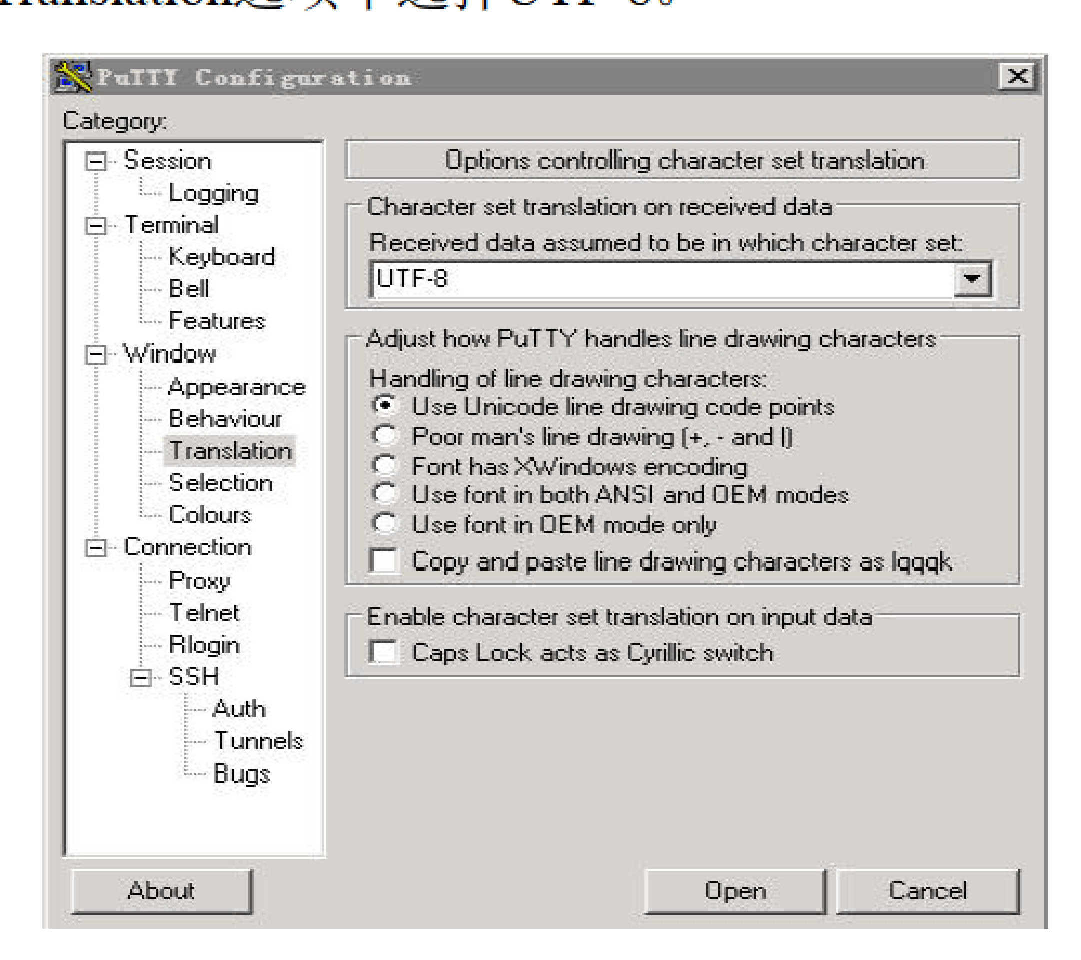



再次开启检查Choose a Tool，看看是否有变化。

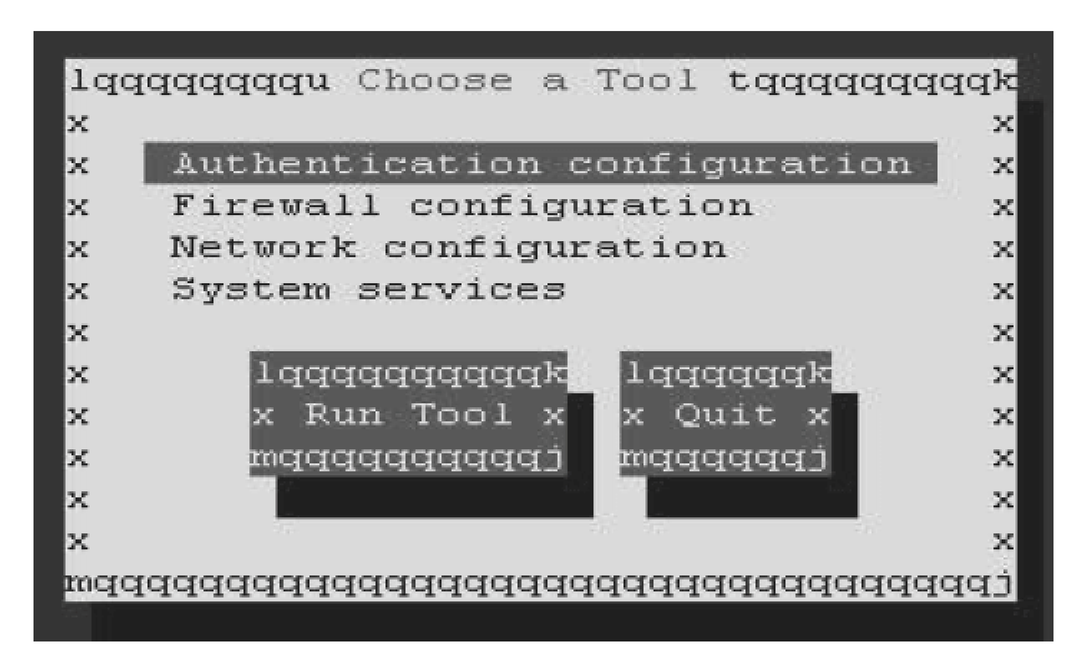
| | |
|---|---|
| **优点** | 能够快速设置 |
| **缺点** | 无法使用 Firewall configuration |

## 方法二

使用PuTTY工具在Translation选项中选择UTF-8。



再次开启PuTTY远程连接工具使用Choose a Tool，看看是否有变化。




| | |
|---|---|
| **优点** | 所有功能不受限制 |
| **缺点** | 登录时要设置，界面有乱码 |

## 方法三

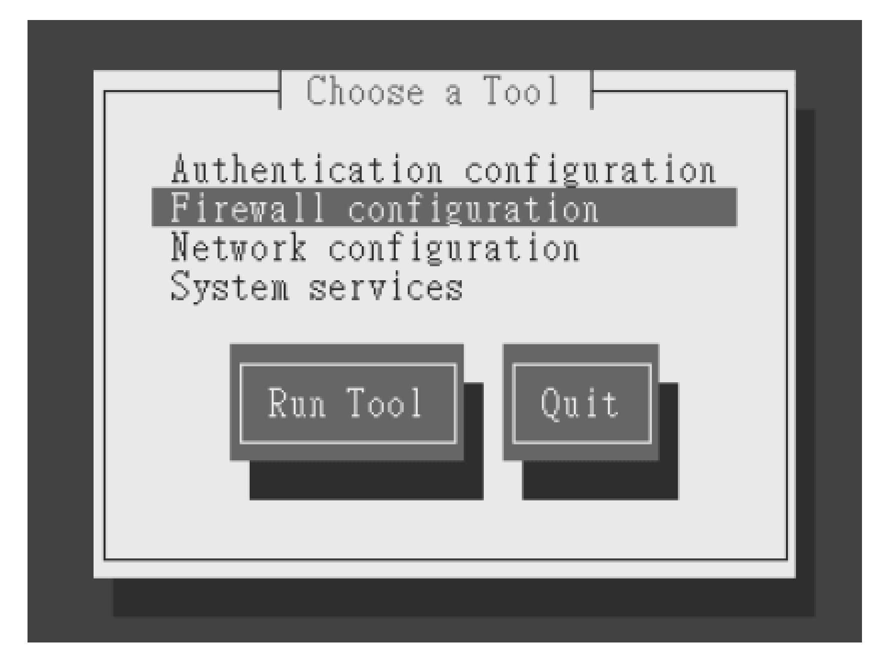
编辑系统默认使用语言的配置文件/etc/sysconfig/i18n，在配置文件中加入 en_US.Big5和zh_CN.UTF-8字符集的结果是不一样的，以下是加入两种字符集的示例，这种设置方式要重新启动才会生效。编辑i18n加入en_US.Big5。

```
[root@localhost ~]# vi /etc/sysconfig/i18n
LANG="en_US.UTF-8"
LANG="en_US.Big5"                                    //加上 en_US.Big5 字符集
SYSFONT="latarcyrheb-sun16"
```

加上LANG="en_US.Big5"登录时会出现错误信息，但是可以正常使用。

```
login as: root
root@192.168.233.229's password: *********
Last login: Wed Aug 24 23:01:53 CST 2012 from 192.168.9.69
check system
-bash: warning: setlocale: LC_CTYPE: cannot change locale (en_US.Big5) : No such file or directory
-bash: warning: setlocale: LC_COLLATE: cannot change locale (en_US.Big5) : No such file or directory
-bash: warning: setlocale: LC_MESSAGES: cannot change locale (en_US.Big5) : No such file or directory
-bash: warning: setlocale: LC_NUMERIC: cannot change locale (en_US.Big5) : No such file or directory
```

再次开启使用Choose a Tool工具，看看是否有变化。

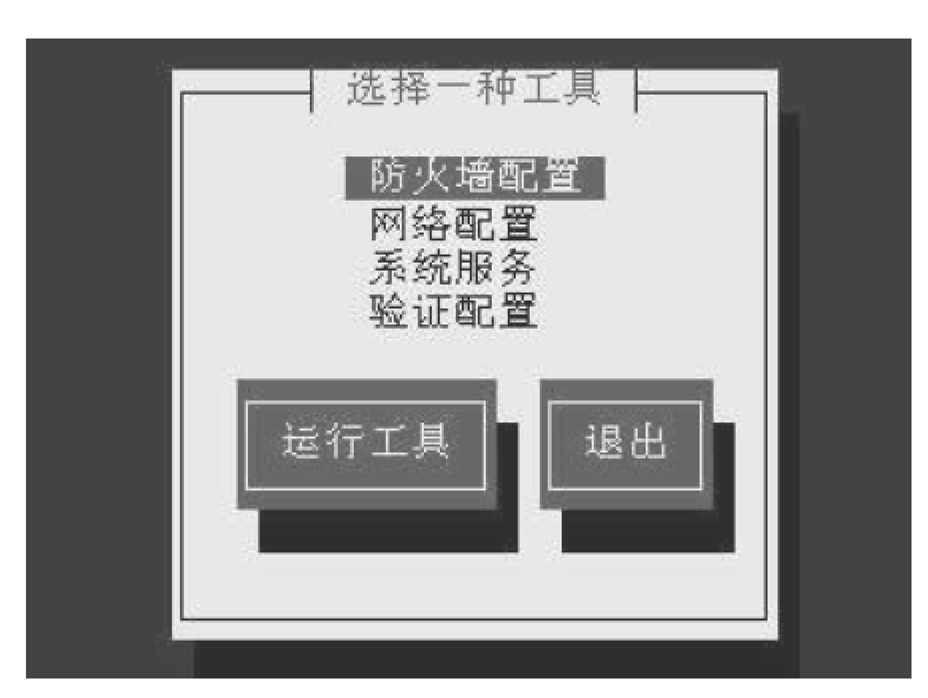



| | |
|---|---|
| **优点** | 界面整洁 |
| **缺点** | 无法使用 Firewall configuration |

下面编辑i18n加入zh_CN.UTF-8

```
[root@localhost ~]# vi /etc/sysconfig/i18n
LANG="en_US.UTF-8"
LANG="zh_CN.UTF-8"                    //加上 zh_CN.UTF-8 字符集会变成简体中文
SYSFONT="latarcyrheb-sun16"
```

再次开启Choose a Tool工具，看看是否有变化。




| | |
|---|---|
| **优点** | 所有功能皆可使用，界面整洁 |
| **缺点** | 原本英文字符集就会变成中文字符集 |

在上述方式中选择其一设置后，再次开启文本模式设置（Choose a Tool）工具，界面就会正常显示。三种方式各有优缺点，请根据需求选择。

## 4.7 查询Linux内核与发行版信息

如何查询Linux内核信息及发行版信息是很重要的，这是因为软件安装时要区分i386的32位平台和x86_64的64位平台，所以一定要掌握相关信息，其实不只是单纯要知道操作系统版本，还有很多信息是有意义的。

若要查询Linux内核信息，利用uname命令可以看到最完整的内核信息。

```
[root@localhost ~]# uname -a
```

```
Linux localhost.localdomain 2.6.32-71.el6.x86_64 #1 SMP Fri May 20 03:51:51 BST 2011 x86_64
x86_64 x86_64 GNU/Linux
```

参数不一样可以查询到的信息就不一样，可按需求查询。

| 参数 | 说明 |
|---|---|
| -a | 输出所有信息 |
| -s | 显示内核名称（Linux） |
| -n | 显示完整主机名称（localhost.localdomain） |
| -r | 显示内核版本（2.6.32-71.el6.x86_64） |
| -v | 显示内核发行日期（#1 SMP Fri May 20 03:51:51 BST 2011） |
| -m | 显示机器硬件类型（x86_64） |
| -p | 显示处理器类型（x86_64） |
| -i | 显示硬件平台类型（x86_64） |
| -o | 显示操作系统（GNU/Linux） |

说明

内核=kernel

查询发行版信息，主要是查看当前操作系统类型版本。

```
[root@localhost ~]# cat /etc/*-release
CentOS Linux release 6.0 (Final)
```

Red Hat系列查询发行版信息使用以下命令。

```
[root@localhost ~]# cat /etc/redhat-release
CentOS Linux release 6.0 (Final)
```

其他方式查询发行版信息，与uname命令类似。

```
[root@localhost ~]# cat /proc/version
Linux version 2.6.32-71.el6.x86_64(mockbuild@c6b6.centos.org) (gcc version 4.4.4 20100726
(Red Hat 4.4.4-13) (GCC) ) #1 SMP Fri May 20 03:51:51 BST 2011
```

## 4.8 查询操作系统应用平台（32位或64位）

查询Linux操作系统应用平台是非常重要的，以免在使用rpm方式安装软件时，才发现软件版本不符合系统应用平台，大多数人都知道使用uname命令去查询，但是看起来眼花缭乱，如何使用最简单的方式查询呢？以下示例能够识别32位或64位的操作系统。

在64位应用平台使用uname命令查询，再使用getconf命令查询64位操作系统，进行对比看是否一样。

```
[root@localhost ~]# uname -a
```

```
Linux localhost.localdomain 2.6.32-71.el6.x86_64 #1 SMP Fri May 20 03:51:51 BST 2011 x86_64
x86_64 x86_64 GNU/Linux
[root@localhost /]# getconf LONG_BIT
64                  //显示为 64 位
```

在32位应用平台使用uname命令查询，再使用getconf命令查询32位操作系统，进行对比看是否一样。

```
 [root@localhost ~]# uname -a
Linux localhost.localdomain 2.6.9-5.ELsmp #1 SMP Wed Jan 5 19:30:39 EST 2005 i686 i686 i386
GNU/Linux
[root@localhost ~]# getconf LONG_BIT
32                  //显示为 32 位
```

# 4.9 查看文件系统类型

使用操作系统时，首先要知道文件系统的类型，如Windows就有NTFS、FAT32、FAT，Linux有ext2、ext3等多种类型的文件系统，使用CentOS 6.0操作系统时文件系统类型默认为ext4，如何查询当前文件系统类型呢？有以下两种方法。

第一种方法是使用mount命令，可以看到文件系统类型为ext4格式。

```
[root@localhost ~]# mount
/dev/mapper/VolGroup-lv_root on / type ext4 (rw)  //分区显示类型
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/sda1 on /boot type ext4 (rw)                 //分区显示类型
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
```

第二种方法是查看fstab表，可以看到文件系统类型为ext4格式。

```
[root@localhost ~]# vi /etc/fstab
#
# /etc/fstab
# Created by anaconda on Wed Aug 17 23:46:05 2011
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab (5) , findfs (8) , mount (8) and/or blkid (8) for more info
#
/dev/mapper/VolGroup-lv_root / ext4  defaults 1 1  //分区显示类型
UUID=b06a6ec6-23da-4905-b7bb-d93ca04aeffc /boot  ext4    defaults     1 2
/dev/mapper/VolGroup-lv_swap swap                swap    defaults     0 0
tmpfs                   /dev/shm                 tmpfs   defaults     0 0
devpts                  /dev/pts                 devpts gid=5,mode=620 0 0
sysfs                   /sys                     sysfs    defaults    0 0
proc                    /proc                    proc     defaults    0 0
```

目前CentOS操作系统的最新文件系统类型为ext4，CentOS 6.0以前的操作系统要使用ext4文件系统类型需要手动转换，CentOS 5以前的操作系统文件类型默认为ext3。

# 4.10 删除操作历史命令

CentOS操作系统在使用命令操作时，系统默认会记录使用过的操作命令，在实际的系统管理中，尽量不要保留这些操作命令历史，将所有操作命令历史删除，这样系统才有安全保障。

使用History命令可以查看所使用过的操作命令。

```
[root@localhost ~]# history  |more   //加上 more 可以一段一段地显示
    1  setup
    2  LANG=CN
    3  setup
    4  clear
    5  yum install httpd
    6  vi /etc/sysconfig/iptables
```

要删除以前所使用过的操作命令，只要加上参数-c，就可以删除这些历史命令了。

```
[root@localhost ~]# history  -c
```

删除历史命令后，要重新启动才会生效，在未重新启动前命令写在buffer中，可以输入【history -w】，这样就可以完全删除所使用过的命令了。

建议将操作系统命令记录的数量减少，HISTSIZE默认为1000行，如果操作过的命令都不想记录，可以改成0，然后重新启动，这样操作命令就不会被记录下来。

```
[root@localhost ~]# vi /etc/profile
HOSTNAME=`/bin/hostname 2>/dev/null`
HISTSIZE=1000         //默认 1000，设为 0 则不会做记录
```

# 4.11 设置服务默认启动或关闭

因为很多系统服务默认系统启动时不自动启动，每次开机后都要使用的服务，必须设置为默认启动，有些没有用到的服务则可以关闭，设置服务默认启动或关闭有图形和命令两种方式，建议使用命令方式去设置，有些服务是无法在图形工具中进行设置的。

## 图形界面设置

先介绍如何使用图形界面进行设置，输入【ntsysv】命令启动Services选项，使用tab及空格键进行选择和修改。




## 命令界面设置

一般来说最常见的设置服务默认启动或默认关闭的方法是命令方式，常用命令是chkconfig，该命令主要是检查、设定系统各服务的运行级别和运行状态，下面以httpd服务为例进行介绍，httpd为Apache服务。

```
[root@localhost ~]# chkconfig httpd on      //将 httpd 服务设为默认启动
[root@localhost ~]# chkconfig --list httpd //查看 httpd 的 level 状态
httpd           0:off    1:off    2:on    3:on    4:on    5:on    6:off
[root@localhost ~]# chkconfig httpd off     //将 httpd 服务设为默认关闭
[root@localhost ~]# chkconfig --list httpd //查看 httpd 的 level 状态
httpd           0:off    1:off    2:off    3:off    4:off    5:off    6:off
```

以上的方式较常见，不过在特殊环境下会设置不同的level启动。下表是chkconfig命令的完整说明。On表示启动，off表示关闭。

| 命令 | 说明 |
|---|---|
| chkconfig --list | 显示所有服务启动情况 |
| chkconfig --add 服务名称 | 增加指定的服务 |
| chkconfig --del 服务名称 | 删除指定的服务 |
| chkconfig --level 0~6 服务名称 on/off | 设置服务 Level 启动/关闭 |

下表为chkconfig 命令显示单个服务的运行状态，默认level 2、3、4、5为on，其他level为off。

| Level | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| on/off | off | off | on | on | on | on | off |

下表说明每个Level所代表的意义。

| Level | 说明 |
| --- | --- |
| 0 | 关机 |
| 1 | 单用户模式 |
| 2 | 多用户命令行模式，没有网络功能 |
| 3 | 多用户命令行模式，有网络功能 |
| 4 | 保留 |
| 5 | 带图形界面的多用户模式 |
| 6 | 重新启动 |

若要将httpd的Level设为0~6都启动，先查看httpd当前的Level设置状态。

```
[root@localhost ~]# chkconfig --list httpd
httpd           0:off    1:off    2:off    3:off    4:off    5:off    6:off
```

使用level参数来设置不同的level，先要将http的level都开启然后都关闭。

```
[root@localhost ~]# chkconfig --level 0123456 httpd on        //全部都开启
[root@localhost ~]# chkconfig --list httpd      //检查 httpd 目前 level 状态
httpd           0:on     1:on     2:on     3:on     4:on     5:on     6:on
[root@localhost ~]# chkconfig --level 0123456 httpd off       //全部都关闭
[root@localhost ~]# chkconfig --list httpd      //检查 httpd 目前 level 状态
httpd           0:off    1:off    2:off    3:off    4:off    5:off    6:off
```

## 4.12 自动开启数字键盘

Windows 开机后Numlock灯是亮着的，使用数字键输入数字比较方便，所以通常都希望开机时就开启数字键盘，如果希望CentOS操作系统开启后Num Lock灯也亮着，需要编辑/etc/rc.local文件，并设置参数，保存退出后，需要重新启动设置才会生效，然后检查系统开机后Numlock灯是否亮着。

```
[root@localhost ~]# vi /etc/rc.local
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
INITTY=/dev/tty[1-8]                      //依序输入以下 4 行，注意有大小写之分
 for tty in $INITTY; do
   setleds -D +num < $tty
done
```

如果不想手工输入，可以输入man setleds查询，约按一次page down就可以看到这些文字，将它们复制到/etc/rc.local文件最后，这样输入一般不会出错。

```
[root@localhost ~]# man setleds
```

```
(without further arguments) will restore the situation in which
the leds reflect the VT flags.

One might use setleds in /etc/rc to define the initial and default
state of NumLock, e.g. by
     INITTY=/dev/tty[1-8]
     for tty in $INITTY; do
          setleds -D +num < $tty
     done
```

## 4.13 CP命令不询问强制复制

cp命令要强制复制就可加上-f或-i，不过都会出现询问窗口，这样就有点不方便。

```
[root@localhost ~]# cp -i install.log /install.log
cp: overwrite `/install.log'? y
[root@localhost ~]#
```

其实有很多方式，不过有些版本不适用，只有在cp前面加一个“\”，这种方式是目前最常用的，可以实现不询问强制复制，下面将install.log复制到根目录的install.log，看看是否需要询问。

```
[root@localhost ~]# \cp  install.log /install.log
```

## 4.14 关闭Ctrl+Alt+Del快捷键防止重新启动

CentOS操作系统只要按下Ctrl+Alt+Del快捷键，系统就会自动重新启动。如果数据正在写入，无意间按下Ctrl+Alt+Del快捷键，不会有任何确认，系统就会直接重新启动，这样会造成很多麻烦，所以要关闭Ctrl+Alt+Del快捷键，以防系统重新启动。

### CentOS 5.x关闭方式

要将Ctrl+Alt+Del快捷键关闭，需要编辑/etc/inittab文件，编辑完成后，必须重新启动，此后不管怎样按Ctrl+Alt+Del快捷键系统都不会重新启动了。

```
[root@localhost ~]# vi /etc/inittab
# Trap CTRL-ALT-DELETE
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now           //默认启用，加上#号关闭
```

### CentOS 6.x关闭方式

按照前面的方式会找不到设置，但是可以设置其配置文件。

```
[root@localhost ~]# vi /etc/inittab
# inittab is only used by upstart for the default runlevel.
#
# ADDING OTHER CONFIGURATION HERE WILL HAVE NO EFFECT ON YOUR SYSTEM.
#
# System initialization is started by /etc/init/rcS.conf
#
# Individual runlevels are started by /etc/init/rc.conf
#
# Ctrl-Alt-Delete is handled by /etc/init/control-alt-delete.conf
      //由此行得知关闭 Ctrl-Alt-Delete 快捷键，需修改 control-alt-delete 配置文件
```

Control-alt-delete.conf文件只有CentOS 6.0才有，CentOS 5.x无法依此设置。

```
[root@localhost ~]# vi /etc/init/control-alt-delete.conf
# control-alt-delete - emergency keypress handling
#
# This task is run whenever the Control-Alt-Delete key combination is
# pressed.  Usually used to shut down the machine.
start on control-alt-delete
#exec /sbin/shutdown -r now "Control-Alt-Delete pressed"  //默认启用，加上#号关闭
```

## 4.15 更改默认登录模式

在CentOS 6.x操作系统以前，只要有安装图形界面，默认登录方式就是图形界面，在CentOS 6.x以后，如果是安装Basic Server，那么就没有图形界面，在/etc/inittab中查看目前开机模式数字一定是3，请根据实际需求设置并确认是否已安装图形界面，如果没有安装，就算将数值设成5，开机也不会进入图形界面。

```
[root@localhost ~]# vi /etc/inittab
# inittab is only used by upstart for the default runlevel.
# ADDING OTHER CONFIGURATION HERE WILL HAVE NO EFFECT ON YOUR SYSTEM.
# System initialization is started by /etc/init/rcS.conf
# Individual runlevels are started by /etc/init/rc.conf
# Ctrl-Alt-Delete is handled by /etc/init/control-alt-delete.conf
# Terminal gettys are handled by /etc/init/tty.conf and /etc/init/serial.conf,
# with configuration in /etc/sysconfig/init.
# For information on how to write upstart event handlers, or how
# upstart works, see init(5), init(8), and initctl(8).
# Default runlevel. The runlevels used are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
id:3:initdefault:   //默认为 3 文本模式，图形界面为 5
```

下表说明了各个代号所代表的意义。

| 代号 | 说明 |
|---|---|
| 0 | Halt：关机 |
| 1 | 单用户模式（如果忘记 root 密码，这是补救的方式之一） |
| 2 | 多用户模式，没有网络功能，不支持 NFS 功能 |
| 3 | 多用户模式，有网络功能，支持 NFS 功能 |
| 4 | unused：这个 run-level 目前尚未定义使用 |
| 5 | X11：启动 X Windows，窗口界面 |
| 6 | Reboot：重新启动 |

# 4.16 关闭SELinux方式

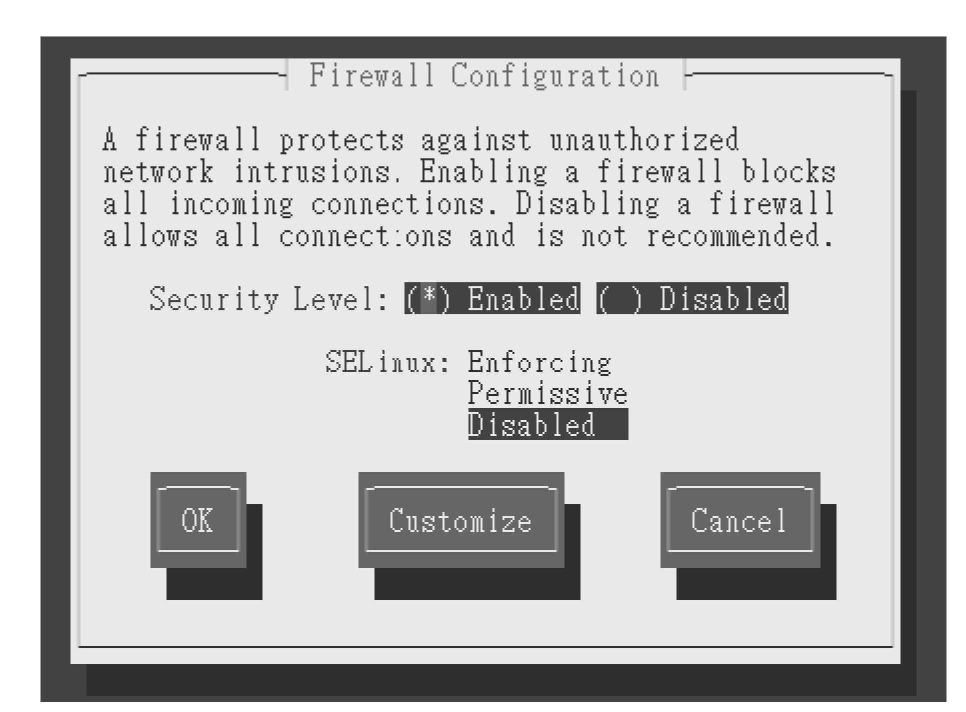
SELinux（Security-Enhanced Linux）是Linux的一种强制访问控制（mandatory access control）体系。它的做法是以最小权限原则（principle of least privilege）为基础，在Linux内核中使用Linux安全模块（Linux Security Modules）。它并非Linux发行版，而是一组可以使用在类Unix操作系统（如Linux、BSD等）中的设置。

SELinux已经被整合到2.6版本的Linux内核之中，独立的修补程序也已经不需要了。其关闭方式共有4种，请根据需求进行设置。

```
[root@localhost ~]# getenforce              //查看 SELinux 运行状态
Enforcing                                   //Enforcing 为开启，disabled 为关闭
```

## 方式一

此方式适用于CentOS 5.x以前的版本，CentOS 6.x之后这种方式就不再使用了，输入【system-config-securitylevel】，将SELinux选为Disabed，然后按【OK】退出界面。




## 方式二

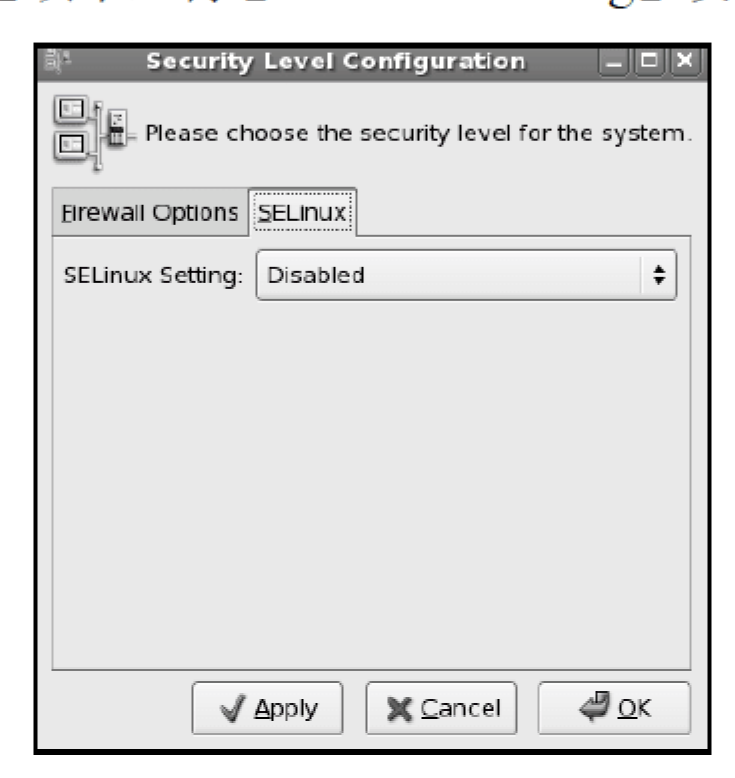
编辑SELinux配置文件，将SELinux设为disabled，则关闭了SELinux。

```
[root@localhost ~]# vi /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled   //默认 enforcing 为开启，disabled 为关闭
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

## 方式三

此方式要安装图形界面才可以使用，选择【System】→【Administration】→【Security Level And Firewall】，在【SELinux】选项中，将【SELinux Setting】设为【Distabled】，然后按【OK】。




## 方式四

使用setenforce命令，只能实现暂时开启或关闭的功能，输入【setenforce 0】为暂时关闭，输入【setenforce 1】为暂时开启。如果要更完整地关闭，建议修改Linux内核参数（Kernel Parameter），并加上【selinux=0】，如果要开启则删除【selinux=0】。这种方式不是每种Linux都适用。

```
[root@localhost ~]# vi /boot/grub/menu.lst
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/mapper/VolGroup-lv_root
#          initrd /initrd-[generic-]version.img
```

```
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.32-71.el6.x86_64)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-71.el6.x86_64 ro root=/dev/mapper/VolGroup-lv_root
rd_LVM_LV=VolGroup/lv_root rd_LVM_LV=VolGroup/lv_swap rd_NO_LUKS rd_NO_MD rd_NO_DM
LANG=en_US.UTF-8 SYSFONT=latarcyrheb-sun16 KEYBOARDTYPE=pc KEYTABLE=us crashkernel=auto
rhgb quiet selinux=0          //加上 selinux=0，完全关闭，开启则删除 selinux=0
        initrd /initramfs-2.6.32-71.el6.x86_64.img
```

总结上述4种方式，建议使用第二种方式，设置完成后，必须重新启动，这样所做的设置才会完全加载。

重新启动后，再次检查 SELinux 运行状态是否已经关闭。

```
[root@localhost ~]# getenforce
Disabled
```

## 4.17 解决CentOS简体中文乱码问题

安装好CentOS操作系统后，如果默认安装字符集为en_US，那么做任何操作，信息显示都会是英文，例如重新启动httpd服务也显示英文。

```
[root@localhost ~]# service httpd restart
Stopping httpd:                                           [  OK  ]
Starting httpd:                                           [  OK  ]
```

查看目录内的中文文件也会显示乱码，所以必须做一些设置让系统可以显示中文。

```
[root@localhost tmp]# ll
total 276
-rw-r--r-- 1 root root 279552 Jul 16  2009 ?t?艮[?c?d??.ppt
```

若要显示简体中文，需要编辑i18n文件，必须将字符集改成zh_CN.UTF-8，还要加上所有支持的字符集，这样保存后，重新启动系统就可以支持简体中文名称了。

```
[root@localhost ~]# vi  /etc/sysconfig/i18n
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-8:zh_CN.GB2312:zh_CN:zh:en_US.UTF-8:en_US:en"
SYSFONT="latarcyrheb-sun16"
```

再次查看中文文件，可以识别简体中文文件名。

```
[root@localhost tmp]# ll
总计 276
```

```
-rw-r--r-- 1 root root 279552 2011-07-16 02:30 系统架构模板.ppt
```

看看重启服务操作是否会改变，检查重新启动httpd服务也会显示简体中文。

```
[root@localhost ~]# service httpd restart
正在停止 httpd:                                              [  确定  ]
正在启动 httpd:                                              [  确定  ]
```

不过在文本模式可以显示简体中文后，再切换X-Windows，文字就有可能都会变成无法识别的方块。



这是因为虽然将字符集改成简体中文，但是系统安装时没有安装简体中文的字体，所以会无法显示，就像Windows系统没有新细明体，也会出现这样的情况，所以必须安装简体中文字体，输入【yum install fonts-chinese】，进行安装，建议也安装fonts-ISO8859-2、fonts-ISO8859-2-100dpi、fonts-ISO8859-2-75dpi。

CentOS操作系统重新启动后，X-Windows就会完全显示简体中文，不过此方式只适合CentOS 5.x。




## 4.18 解决32位CentOS系统支持大内存

CentOS操作系统在x86的硬件平台下，内存通常只能读取到3GB左右，Windows XP也只能读取3GB多，最新的Windows 7 x86也刚刚能读取3GB，其他版本的Linux系统也是一样，CentOS

x86系统也是3GB，目前服务器上的内存容量都很大，很容易就可以达到3GB以上，所以需要将内存支持度再扩大，下列做法可以将内存容量超过3GB以上。

检查目前内存容量，CentOS x86系统安装4GB的内存，在系统中输入【free -m】，所看到的内存容量只有3GB（3034MB），必须更新内核才可以支持到4GB。

```
[root@localhost ~]# free -m
             total       used       free     shared    buffers     cached
Mem:          3034        218       2816          0         51        119
-/+ buffers/cache:         46       2987
Swap:         2047          0       2047
```

使用yum在线更新，可以让内核支持更大的内存容量，如果要全部更新kernel是有风险的，有可能无法开机，建议不要更新全部的kernel，不能输入【yum install kernel*】这样的命令，这样操作无法开机是正常的，建议更新前备份数据。当前为CentOS 5.6 i386系统更新支持大内存的软件为kernel-PAE 2.6.18，更新版本以所安装的系统版本为主。

```
[root@localhost ~]# yum install kernel-PAE
========================================================================
 Package                Arch      Version               Repository     Size
========================================================================
Installing:
 kernel-PAE           i686        2.6.18-274.3.1.el5     updates     18 M
Transaction Summary
========================================================================
```

编辑配置文件，更新完内核后，编辑grub.conf。默认为defult=1，将之设为defult=0，目的是让kernel-PAE默认在内核中启动。

```
[root@localhost ~]# vi /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol00
#          initrd /initrd-version.img
#boot=/dev/sda
default=0      //默认为 defult=1 关闭，0 为开启
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.18-274.3.1.el5PAE)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-274.3.1.el5PAE ro root=/dev/VolGroup00/LogVol00
        initrd /initrd-2.6.18-274.3.1.el5PAE.img
title CentOS (2.6.18-238.el5)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-238.el5 ro root=/dev/VolGroup00/LogVol00
```

```
        initrd /initrd-2.6.18-238.el5.img
```

设置完成后，重新启动操作系统才会生效。

```
[root@localhost ~]# shutdown -r now
Broadcast message from root (pts/0) (Thu Oct  6 19:45:53 2012) :
The system is going down for reboot NOW!
```

重新启动后再查看系统内存是否超过4G，输入【free -m】，系统显示超过4G。

```
[root@localhost ~]# free -m
             total       used       free     shared    buffers     cached
Mem:          5939        179       5759          0         13        119
-/+ buffers/cache:         46       5892
Swap:         2047          0       2047
```

CentOS 6.x操作系统已解除PAE限制，所以支持4GB以上的内存。不过，如果要使用大容量内存，最好还是选择x86_64版本，系统功效也比i386好。

# 第二部分

# 服务器配置篇

# 第 5 章

# Apache——网站服务器

Apache 网站服务器软件官方网站：http://httpd.apache.org/。

Apache HTTP Server（简称Apache）是Apache软件基金会开放源代码的Web服务器软件，因为可以在大多数操作系统上运行，且可以跨平台和安全性比较高，所以被广泛使用，是目前最流行的Web服务器端软件之一。支持的网页语言也很多，如PHP、JSP等。Apache目前为Linux系统默认的Web服务器软件。

## 5.1 安装 Apache服务

### 安装Apache软件 [yum方式]

Apache软件通常会以yum在线更新方式进行安装，下面首先介绍如何使用yum在线更新方式进行安装，后面会介绍如何使用源代码编译方式进行安装。

```
[root@localhost ~]# yum install httpd -y
Dependencies Resolved
========================================================================
 Package            Arch        Version                 Repository     Size
========================================================================
Installing:
 httpd              x86_64      2.2.15-5.el6.centos     base           811 k
Installing for dependencies:
 apr                x86_64      1.3.9-3.el6_0.1         updates        124 k
 apr-util           x86_64      1.3.9-3.el6_0.1         updates        87 k
 apr-util-ldap      x86_64      1.3.9-3.el6_0.1         updates        15 k
 httpd-tools        x86_64      2.2.15-5.el6.centos     base           68 k

Transaction Summary
========================================================================
Install       5 Package (s)
```

```
Upgrade       0 Package(s)

Total download size: 1.1 M
Installed size: 3.5 M
```

## 配置防火墙

Apache服务默认使用80端口，为了使Apache服务能够对外正常提供服务就必须在防火墙配置中开启80端口。

```
[root@localhost ~]# vi /etc/sysconfig/iptables              //编辑 iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
                                                            //Apache 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

## 启动Apache服务

Apache配置完成后，即可启动服务，并将Apache服务配置为系统默认启动。

```
[root@localhost ~]# service httpd start
Starting httpd:                                            [  OK  ]
[root@localhost ~]# chkconfig  httpd on
```

CentOS 6.x以前版本安装完Apache服务后启动不会出现任何错误信息，CentOS 6.x启动时就会出现没有配置ServerName参数的警告信息，但不影响运行。

```
[root@localhost ~]# service httpd start  //没有配置 ServerName 启动的警告信息
```

```
Starting httpd: httpd: Could not reliably determine the server's fully qualified domain
name, using localhost.localdomain for ServerName  [  OK  ]
```

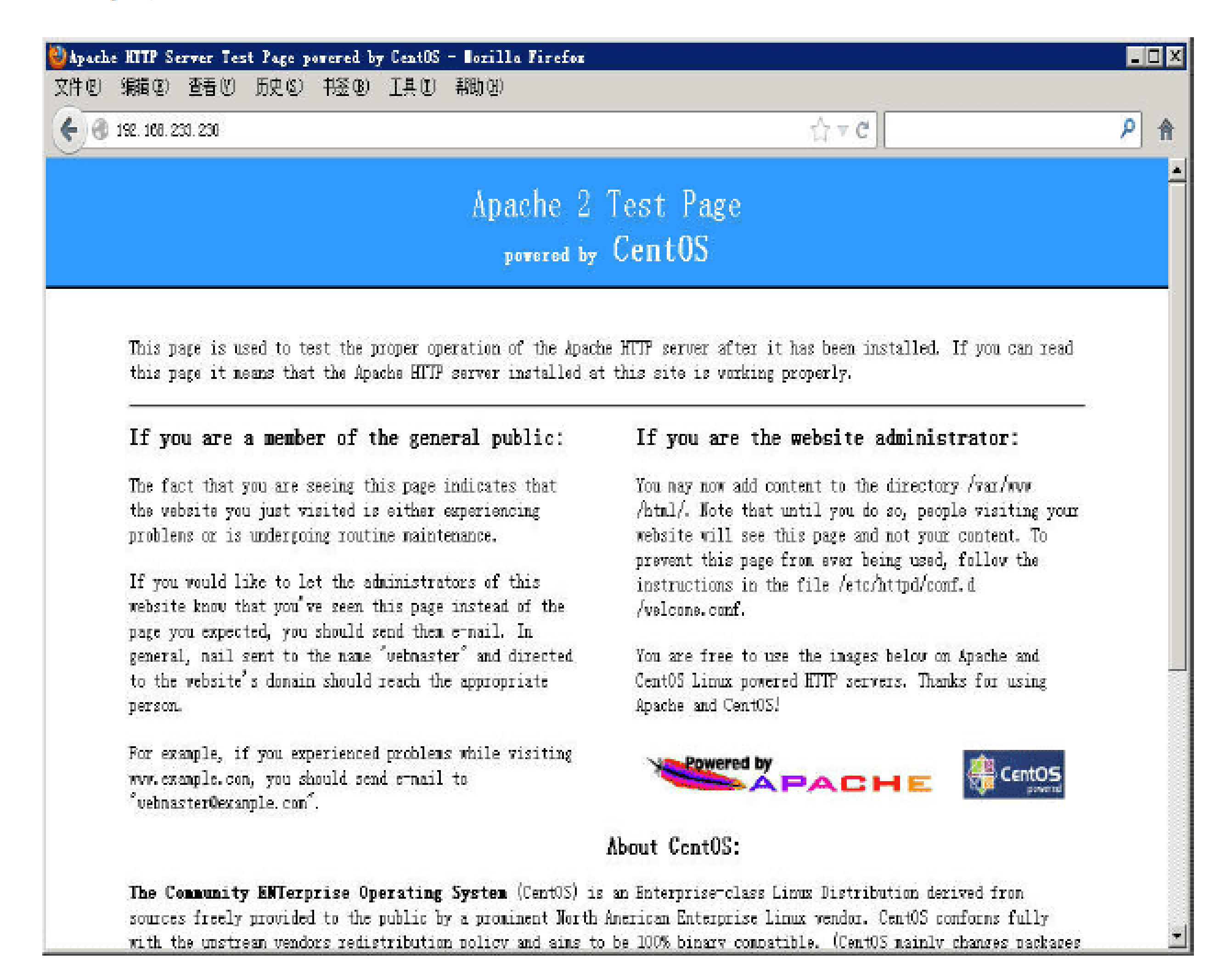
## Apache命令说明

Apache服务最常用的命令就是启动、关闭、重新启动，还有查看目前启动状态。

| 命令 | 命令说明 |
|---|---|
| service httpd start | 启动 Apache 服务 |
| service httpd stop | 关闭 Apache 服务 |
| service httpd restart | 重新启动 Apache 服务 |
| service httpd ststus | 查看 Apache 服务运行状态 |

## 测试范例网页

在浏览器中输入【http://IP或网址】，正常启动的Apache默认网页如下图所示，此为CentOS操作系统默认Apache网页。




# 5.2 配置Apache服务

Apache配置文件的默认路径为：/etc/httpd/conf/httpd.conf，这个路径是以yum方式安装的，如果以源代码手动编译方式安装，路径则可以指定到安装目录。以下几个配置是较为常见的，有关完整的说明请参考Apache官方网站：http://httpd.apache.org/docs/2.2/mod/directives.html。

> **说明**
>
> Apache配置文件修改过后都需要重新启动Apache服务，否则配置不会生效。

## 连接时间

此功能是指如果连接空闲时间过长的话，会中断连接，可根据情况配置。

```
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf     //编辑 Apache 配置文件
Timeout 60                   //接收或发送，当持续连接等待超过 60 秒则该连接就中断
```

## 配置字符集

网页字符集默认有Big5或UTF-8，请根据需求配置，另外建议如果可以选择网页编码，尽量选择UTF-8。

```
# Specify a default charset for all content served; this enables
# interpretation of all content as UTF-8 by default.  To use the
# default browser choice (ISO-8859-1), or to allow the META tags
# in HTML content to override this choice, comment out this
# directive:
#
AddDefaultCharset UTF-8              //配置文件默认字符集编码为 UTF-8,
```

## 配置索引页面

假设网站的索引页面是index.php，如果只是输入【http://IP或网址/】，没有输入【http://IP或网址/index.php】，是不能正常显示index.php内容的，因为索引页面默认为index.html、index.html.var，建议修改配置文件，添加index.php并将它放置在index.html前面。CentOS操作系统环境下index.php已默认为索引页面。

```
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
# The index.html.var file (a type-map) is used to deliver content-
# negotiated documents.  The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
DirectoryIndex index.php index.htm index.html index.html.var //默认索引页面
```

## 配置网页主目录

DocumentRoot参数是网页存放的主目录，CentOS 6.x目录路径为/var/www/html，此路径为yum方式安装的配置，以源代码编译方式安装可以指定目录的路径。

```
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
```

```
#
DocumentRoot "/var/www/html"                                    //网页默认存放的目录
```

## 配置连接端口

在网站对外提供访问时，使用的端口默认为80，默认情况下Apache会在所有IP地址上监听。Listen是一个必须设置的参数。如果修改指定的端口，也必须将防火墙的端口修改。

```
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, in addition to the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen 80                                                          //Apache 监听端口
```

## 配置ServerName

ServerName主要用于识别主机名称和端口，默认不用配置，但是CentOS 6.x必须要配置，如果暂时不知道对外提供服务的主机名称，只要将该行#号删除即可。

```
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.  See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
ServerName www.example.com:80     //默认不使用#号，CentOS 6.0 版本后必须要配置。
```

## 配置KeepAlive传输请求

KeepAlive传输请求在Apache配置文件中默认为关闭，建议设为On。比如在同一时间发送多个连接，on的状态下可以使用一个TCP发送，如果是off状态下，则会以多个TCP连接，影响网络效率。

```
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection) . Set to "Off" to deactivate.
#
```

```
KeepAlive on     //此配置默认为 off，建议设为 on
```

## 配置MaxKeepAliveRequests连接数

MaxKeepAliveRequests在Apache配置文件中默认为100个连接数，该参数限制了当启用KeepAlive时，每个连接允许的请求数量，如果主机效率不错建议设高一点，不过尽量不要超过100太多，连接数过多也会降低效率。设为0的话，则连接数就不受限制，但建议不要这样配置。

```
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100
```

# 5.3 源代码安装Apache

Apache 网站服务软件官方下载地址：http://httpd.apache.org/download.cgi。

目前Apache都是以rpm包或yum在线更新安装，其实也没指定用什么方法安装，不过发现有些人配置环境时会使用源代码编译安装，因为rpm包、yum在线更新与源代码编译安装的路径不一样，所以初学者比较不容易掌握，毕竟灾难还原时都是直接将文件还原到原路径，如果以rpm或yum安装，那在还原数据时就要修改路径，所以学会怎样进行源代码安装是有必要的。

## 下载Apache 2.2压缩文件

使用wget方式下载Apache压缩文件，或下载后使用WinSCP工具上传压缩文件。

```
[root@localhost ~]# wget  http://mirror.bit.edu.cn/apache//httpd/httpd-2.2.22.tar.gz
--2012-08-26 21:04:34--  http://mirror.bit.edu.cn/apache//httpd/httpd-2.2.22.tar.gz
Resolving mirror.bit.edu.cn... 219.143.204.117
Connecting to mirror.bit.edu.cn|219.143.204.117|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7200529 (6.9M) [application/octet-stream]
Saving to: `httpd-2.2.22.tar.gz.1'
100%[======================================>] 7,200,529    245K/s   in 43s
2012-08-26 21:06:01 (163 KB/s) - "httpd-2.2.22.tar.gz"saved [7200529/7200529]
```

> **说明**
>
> 最新版本请以Apache官方网站提供的信息为主。

## 编译安装Apache 2.2

因源代码包一般为压缩文件，所以在下载成功后，需先把Apache压缩文件解压缩，然后进行编译安装Apache。

```
[root@localhost ~]# tar -zxvf httpd-2.2.*.tar.gz  //解压缩文件
…中间省略…
[root@localhost ~]# cd  httpd-*                    //进入解压缩目录
[root@localhost httpd-2.2.22]#./configure          //检查安装平台是否支持安装
…中间省略…
[root@localhost httpd-2.2.22]#make                 //根据安装平台进行编译
…中间省略…
[root@localhost httpd-2.2.22]#make install        //安装软件
…中间省略…
```

> **说明**
>
> 如果使用源代码编译安装，记住上述三个命令，源代码文件安装方式都大同小异。编译时若出现C compiler found错误，代表缺少gcc软件，输入【yum install gcc】进行安装。
>
> ```
> configure: error: in `/root/httpd-2.2.22/srclib/apr':
> configure: error: no acceptable C compiler found in $PATH
> See `config.log' for more details.
> configure failed for srclib/apr
> ```

## 配置防火墙

使用Apache服务必须在防火墙配置中开启端口80，这样Apache才能对外服务。

```
[root@localhost ~]# vi /etc/sysconfig/iptables          //编辑 iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
                                                       //开放 Apache 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
```

```
iptables: Flushing firewall rules:                          [  OK  ]
iptables: Setting chains to policy ACCEPT: filter           [  OK  ]
iptables: Unloading modules:                                [  OK  ]
iptables: Applying firewall rules:                          [  OK  ]
```

## Apache apachectl命令说明

下面是Apache最常使用的命令，这些命令与Yum方式安装的Apache不一样。

| 操作说明 | 操作方式 |
|---|---|
| 启动 Apache | /usr/local/apache2/bin/apachectl start |
| 停止 Apache | /usr/local/apache2/bin/apachectl stop |
| 重新启动 Apache | /usr/local/apache2/bin/apachectl restart |
| 重新启动 Apache，原有连接不中断 | /usr/local/apache2/bin/apachectl graceful |
| 显示 Apache 运行状态 | /usr/local/apache2/bin/apachectl status |
| 显示 Apache 服务器完整状态 | /usr/local/apache2/bin/apachectl fullstatus |
| 检查 Apache 配置文件是否正确 | /usr/local/apache2/bin/apachectl configtest |
| 显示 Apache 说明 | /usr/local/apache2/bin/apachectl help |

## Apache目录说明（源代码编译安装）

以源代码编译安装，默认路径是/usr/local，相关目录说明请参考下表。

| Apache 2 目录路径 | 目录说明 |
|---|---|
| /usr/local/apache2 | Apache 2 主目录 |
| /usr/local/apache2/htdocs | Apache 2 网页存放默认目录 |
| /usr/local/apache2/logs | Apache 2 日志记录文件目录 |
| /usr/local/apache2/conf | Apache 2 配置文件目录 |

## 启动Apache

安装完成后，接下来就是启动Apache网站服务器。

```
[root@localhost ~]# /usr/local/apache2/bin/apachectl start   //启动 Apache
[root@localhost ~]# /usr/local/apache2/bin/apachectl start
                                                  //再启动一次可以看到已经启动
httpd (pid 16067) already running
```

启动时出现ServerName错误信息，表示需要配置ServerName才可以正常启动。

```
[root@localhost httpd-2.2.22]# /usr/local/apache2/bin/apachectl start
httpd: Could not reliably determine the server's fully qualified domain name, using
localhost.localdomain for ServerName
[root@localhost ~]# vi /usr/local/apache2/conf/httpd.conf
#
```

```
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName www.example.com:80        //将该行前#删除后，保存退出并重新启动 Apache
```

## 测试Apache服务器

在浏览器中输入【http://IP或网址】，出现【IT WORKS!】，如下图所示，表示Apache服务启动正常。




# 5.4 支持PHP程序

PHP的应用范围相当广泛，是常见的HTML内嵌式语言，尤其是在Web程序的开发上。一般来说PHP语言大多在Web服务器（Apache）上执行，通过执行PHP程序代码来产生使用者浏览的网页。PHP语言可以在多数的服务器和操作系统上执行，如Windows、Linux等系统，而且PHP完全是免费的，因此受到越来越多人的采用，以下是配置Apache以支持PHP的步骤。

## 检查PHP软件

检查是否安装了PHP软件，如果出现PHP相关软件代表可以支持PHP网页，如果无任何软件，代表尚未安装PHP软件，则无法支持PHP网页。

```
[root@localhost /]# rpm  -qa | grep php    //检查 PHP 软件
php-5.3.3-6.el6_0.1.x86_64
php-cli-5.3.3-6.el6_0.1.x86_64
php-common-5.3.3-6.el6_0.1.x86_64
```

## 安装PHP软件

如果没有安装PHP软件，那就要自动安装了。安装PHP软件的方法很简单，只要以yum在

线更新的方式安装即可。

```
[root@localhost ~]# yum install php  -y                    //PHP 软件安装
=========================================================================
 Package            Arch          Version                   Repository      Size
=========================================================================
Installing:
 php                x86_64        5.3.3-6.el6_0.1           updates         1.1 M
Installing for dependencies:
 php-cli            x86_64        5.3.3-6.el6_0.1           updates         2.2 M
 php-common         x86_64        5.3.3-6.el6_0.1           updates         516 k

Transaction Summary
=========================================================================
Install       3 Package(s)
Upgrade       0 Package(s)

Total download size: 3.8 M
Installed size: 13 M
```

安装完成后，必须重新启动Apache服务，Apache才可以支持PHP语法（每个版本不一定都需要重新启动）。

```
[root@localhost ~]# service httpd restart                  //重新启动 Apache
Stopping httpd:                                             [  OK  ]
Starting httpd:                                             [  OK  ]
```

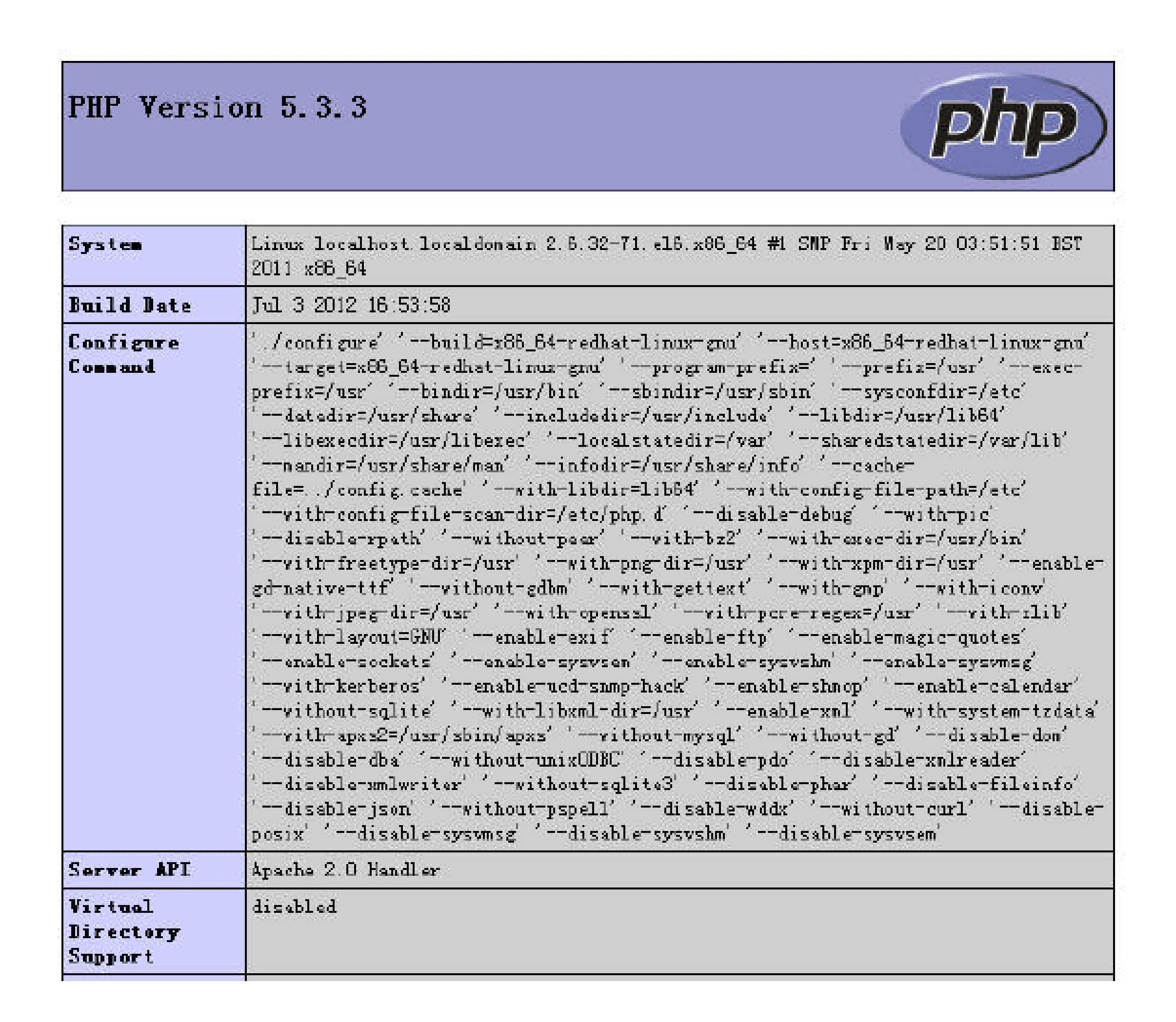
## 测试PHP代码

软件PHP安装确定后，在Apache网页目录中创建一个PHP范例网页index.php，测试是否可以正常显示PHP信息，可以输入PHP查询状态的语法。

```
[root@localhost /]# vi /var/www/html/index.php  //在 Apache 默认目录下创建范例网页
<?php
phpinfo();
?>
```

> **说明**
> Yum在线更新安装Apache的网页默认目录为/var/www/html

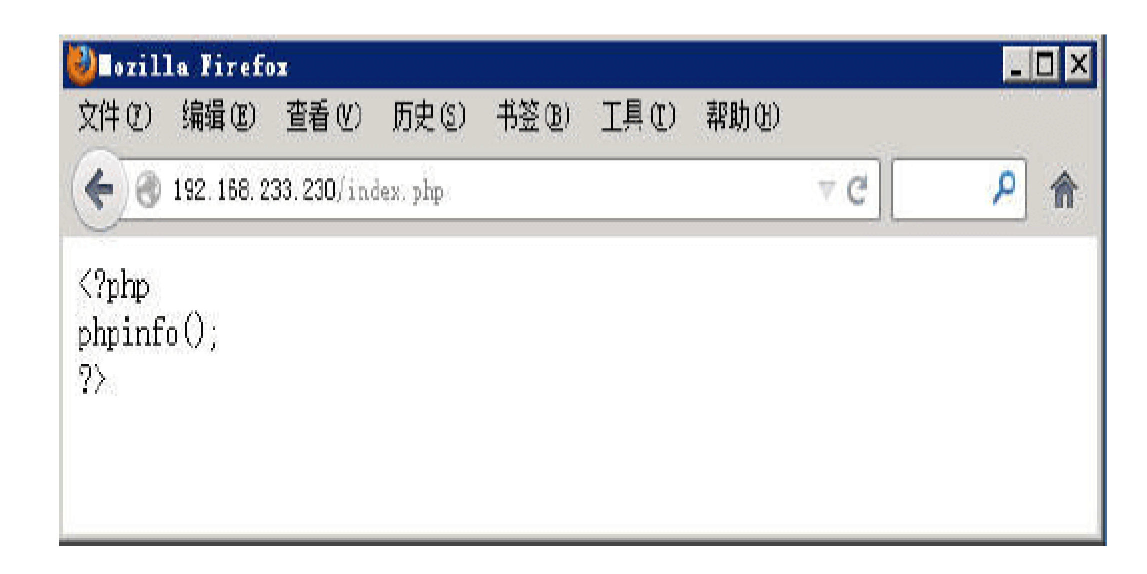
打开浏览器，输入【http://IP或网址/index.php】，下图表示可以正常显示PHP网页。



PHP Version 5.3.3

| | |
|---|---|
| System | Linux localhost.localdomain 2.6.32-71.el6.x86_64 #1 SMP Fri May 20 03:51:51 BST 2011 x86_64 |
| Build Date | Jul 3 2012 16:53:58 |
| Configure Command | './configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--with-kerberos' '--enable-ucd-snmp-hack' '--enable-shmop' '--enable-calendar' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xml' '--with-system-tzdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--disable-dom' '--disable-dba' '--without-unixODBC' '--disable-pdo' '--disable-xmlreader' '--disable-xmlwriter' '--without-sqlite3' '--disable-phar' '--disable-fileinfo' '--disable-json' '--without-pspell' '--disable-wddx' '--without-curl' '--disable-posix' '--disable-sysvmsg' '--disable-sysvshm' '--disable-sysvsem' |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | disabled |

如果出现下图，表示不能支持PHP网页，PHP软件未安装，请重新检查PHP是否已正常安装。




刚才创建的PHP页面是查询PHP状态语法，显示全部的PHP信息，如果不想一次显示多个信息，可以编辑查询页面的参数，修改刚才创建的index.php，可以选择输入名称或参数值。

| PHP 状态语法 | |
|---|---|
| **名称方式** | **参数值** |
| <?php<br>phpinfo（INFO_GENERAL）;<br>?> | <?php<br>phpinfo（1）;<br>?> |

| Phpinfo 语法参数说明 | | |
|---|---|---|
| **名称** | **参数值** | **查询信息** |
| INFO_GENERAL | 1 | 配置 php.ini 位置、创建日期、服务器信息 |
| INFO_CREDITS | 2 | 开发人员使用的资料 |
| INFO_CONFIGURATION | 4 | 目前 PHP 命令的 local 和 master 值 |
| INFO_MODULES | 8 | 加载的模块和其他相应的配置 |
| INFO_ENVIRONMENT | 16 | 环境变量信息 |
| INFO_VARIABLES | 32 | 显示所有默认变量信息 |
| INFO_LICENSE | 64 | PHP 的许可协议 |
| INFO_ALL | -1 | 显示所有数据（默认值） |

说明

INFO_ALL的写法和不加任何参数的写法，显示信息是一样的。

## 开启register_globals

如果在浏览PHP网页时提示输入用户名和密码，但是在输入用户名和密码后，用户还是无法登录，登录界面又回到输入用户名和密码的页面，如下图所示。




原因是新版PHP为了网站安全性考虑，在接收网页传递的全局变量时把register_globalse参数默认设置为关闭状态，低版本则不会有影响，所以必须将register_globalse改成On（默认为Off），这样就不会发生无法登录的情形。

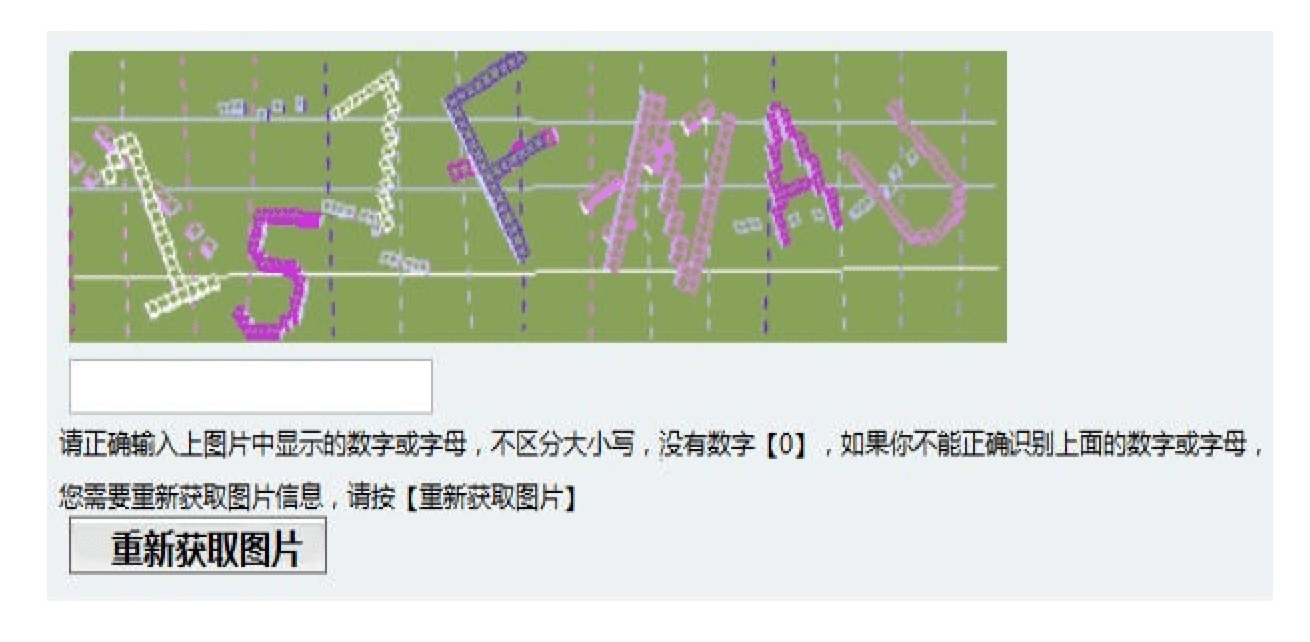
```
[root@localhost /]# vi  /etc/php.ini    //编辑 php 配置文件
……
register_globals = On
```

重新启动Apache服务后，再次输入用户名和密码，PHP网页就不会提示无法登录了。

```
[root@localhost ~]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

## PHP支持图形验证码

所谓图形验证码就是一张图片里有数字及字母，这种功能通常在论坛用户认证登录时使用，图形验证码的功能是防止有人利用程序来大量注册用户，或者是发广告留言等，多了这一层防护，可以减少这些情况的发生，但安装此功能前，必须要安装所需要的软件php-gd。




安装完成后，建议重新启动Apache服务，这样就可以使用图形验证码的功能了。

```
ot@localhost ~]# yum install -y php-gd    //安装 gd 软件
```

```
Dependencies Resolved

==========================================================================
 Package         Arch      Version                 Repository         Size
==========================================================================
Installing:
 php-gd         x86_64     5.3.2-6.el6_0.1          updates          103 k
Installing for dependencies:
 libXpm         x86_64      3.5.8-2.el6              base              59 k

Transaction Summary
==========================================================================
Install       2 Package(s)
Upgrade       0 Package(s)

Total download size: 162 k
Installed size: 446 k
```

## 5.5 phpSysInfo 显示系统信息

官方网站：http://phpsysinfo.sourceforge.net/。

phpSysInfo 是一个能够显示主机系统信息的PHP程序，主要用来检测主机的硬设备信息，包括所用操作系统及内核版本、计算机名称、计算机运行时间、网卡、内存、存储设备的使用情况等。

### 安装PHP软件

phpSysInfo 3版本需要安装Apache及php 5.2版本以上的软件，然后需要安装支持phpSysInfo的应用软件php-mbstring及php-xml，下面检查是否已安装相关软件。

```
[root@localhost ~]# rpm -qa|grep php     //检查 phpSysInfo 所需的软件
php-common-5.3.2-6.el6_0.1.x86_64
php-cli-5.3.2-6.el6_0.1.x86_64
php-xml-5.3.2-6.el6_0.1.x86_64
php-mbstring-5.3.2-6.el6_0.1.x86_64
php-5.3.2-6.el6_0.1.x86_64
```

如果没有安装PHP相关软件，则使用yum在线更新方法进行安装。

```
[root@localhost ~]# yum install -y  httpd php php-mbstring  php-xml

Dependencies Resolved

==========================================================================
 Package           Arch         Version            Repository     Size
==========================================================================
```

```
Installing:
 httpd              x86_64    2.2.15-5.el6.centos     base         811 k
 php                x86_64    5.3.2-6.el6_0.1         updates      1.1 M
 php-mbstring       x86_64    5.3.2-6.el6_0.1         updates      504 k
 php-xml            x86_64    5.3.2-6.el6_0.1         updates      100 k
Installing for dependencies:
 apr                x86_64    1.3.9-3.el6_0.1         updates      124 k
 apr-util           x86_64    1.3.9-3.el6_0.1         updates       87 k
 apr-util-ldap      x86_64    1.3.9-3.el6_0.1         updates       15 k
 httpd-tools        x86_64    2.2.15-5.el6.centos     base          68 k
 libxslt            x86_64    1.1.26-2.el6            base         450 k
 php-cli            x86_64    5.3.2-6.el6_0.1         updates      2.2 M
 php-common         x86_64    5.3.2-6.el6_0.1         updates      516 k

Transaction Summary
=========================================================================
Install      11 Package(s)
Upgrade       0 Package(s)

Total download size: 5.9 M
Installed size: 20 M
```

## 安装phpSysInfo

首先进入/var/www/html网页主目录，下载phpsysinfo文件，可以下载到本地再利用WinSCP工具上传到网页主目录下，也可以在服务器上直接使用wget命令下载，下载完成后解压缩，然后进入phpsysinfo目录，复制模板配置文件config.php.new，并重命名为config.php。

```
[root@localhost ~]# cd /var/www/html  //进入网页主目录
[root@localhosthtml]#wget
http://downloads.sourceforge.net/project/phpsysinfo/phpsysinfo/3.0.13/
phpsysinfo-3.0.13.tar.gz
…中间省略…
[root@localhost html]# tar -zxvf phpsysinfo-*.tar.gz    //解压缩
…中间省略…
[root@localhost html]# cd phpsysinfo     //进入 phpsysinfo 目录
[root@localhost phpsysinfo]# cp config.php.new config.php
                 //复制 phpsysinfo 配置文件
```

配置完成后，重新启动Apache服务。这样phpsysinfo才能正常使用。

```
[root@localhost phpsysinfo]# service httpd start
Starting httpd:                                            [  OK  ]
```

## 配置防火墙

因为phpSysInfo是以Apache网页方式浏览的，所以必须在防火墙配置中开启80端口。

```
[root@localhost phpsysinfo]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
```

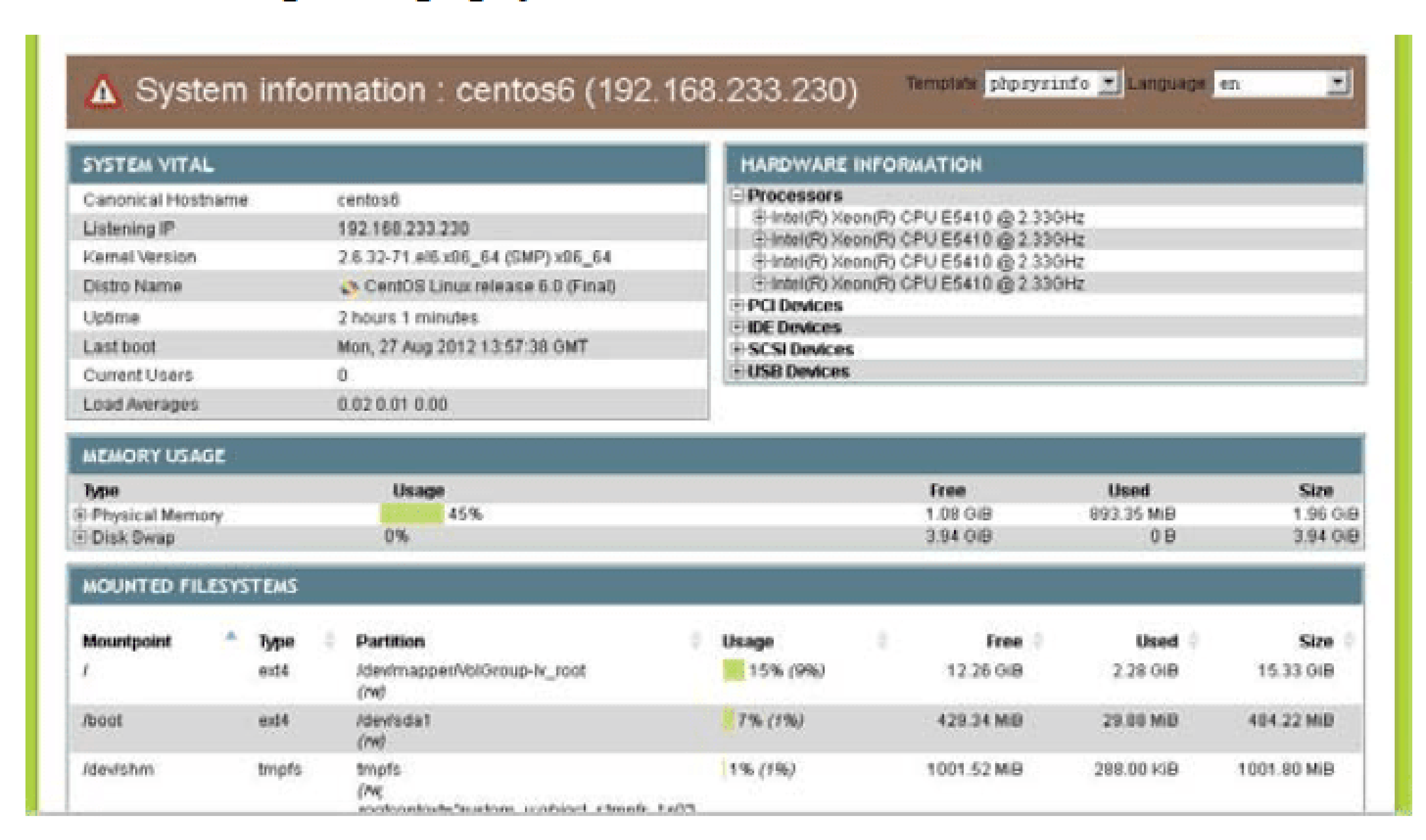
```
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT   //Apache 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

配置完防火墙后，必须重新启动防火墙，配置才会生效。

```
[root@localhost phpsysinfo]# service iptables restart
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

### 测试phpSysInfo

打开浏览器，输入【http://IP/phpsysinfo】，如下图所示，显示系统相关信息。




PhpSysInfo默认语言为英文，可以在Language中选择自己习惯的语言，系统会自动切换语言。




## 5.6 Apache支持CGI

Linux系统常用的网页语言除了PHP外，还有CGI。程序语言 Perl 是一种被广泛用于CGI（Common Gateway Interface）的语言，除Perl外，像Unix shell scripts、Python、Ruby、PHP、

C/C++和Visual Basic都可以用来编写CGI。Apache也可以支持使用CGI，不过配置是关闭的，必须要自行开启配置。

## 开启Apache对CGI的支持

编辑Apache配置文件，删除支持CGI选项前的#号，并在最后加上.pl，以便可以支持pl文件。

```
[root@localhost ~]# vi  /etc/httpd/conf/httpd.conf
# To use CGI scripts outside of ScriptAliased directories:
# (You will also need to add "ExecCGI" to the "Options" directive.)
#
AddHandler cgi-script .cgi .pl   //删除#号才可以支持 cgi
```

配置完成后，重新启动apache服务，配置才会生效。

```
[root@localhost ~]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

## 创建CGI测试网页

CGI文件默认放在/var/www/cgi-bin目录下，先进入该目录，创建一个支持CGI文件的范例，文件名称为hello.cgi，创建完成后，将文件权限修改为755，若权限不修改为755的话，CGI会无法执行。

```
[root@localhost ~]# cd /var/www/cgi-bin        //进入 cgi 网页目录
[root@localhost cgi-bin]# vi hello.cgi         //编辑 cgi 测试网页
#!/usr/bin/perl
print "Content-type: text/html\n\n";
print "Hello!!";
[root@localhost cgi-bin]# chmod 755 hello.cgi
```

## 测试是否支持CGI

打开浏览器，输入【http://IP或网址/cgi-bin/hello.cgi】，执行结果如下图所示，这表示Apache可以支持CGI文件。




若执行结果出现如下图所示的Internal Server Error，有两个可能的原因。

- CGI 页面程序的权限不够，需要配置为 711 或 755。
- 程序中有一行 #!/usr/bin/perl，在#号前不可以有空格。

**Internal Server Error**

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, root@localhost and inform them of the time the error occurred, and anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

---

*Apache/2.2.15 (CentOS) Server at 192.168.233.230 Port 80*

## 5.7 让Apache支持SSL

HTTPS存在不同于HTTP的默认端口及一个加密/身份验证层，HTTPS全名为Hypertext Transfer Protocol over Secure Socket Layer，简单来说就是使用SSL会让网页浏览更安全，Apache默认不支持SSL，必须自行添加配置。

SSL是Web服务器和浏览器之间以加解密方式进行沟通的安全技术标准，这样的沟通过程确保了服务器与浏览器之间传输的数据是完整的，并且确保了服务器的真实性，SSL是一个企业级标准，被网站用来保护它们与客户的在线交易信息，在网络交易或牵涉到机密数据时才使用SSL安全链接，一台Web服务器需要申请一张数字证书，如果要有两台Web服务器，必须再申请一张数字证书。

### 安装mod_ssl模块

首先检查是否已安装SSL软件。

```
[root@localhost ~]# rpm -qa|grep mod_ssl            //检查是否安装 SSL 软件
mod_ssl-2.2.15-5.el6.centos.x86_64
```

如果没有安装mod_ssl模块，Web服务器就无法提供SSL服务，可使用Yum在线更新方式安装。

```
[root@localhost ~]# yum install -y mod_ssl          //安装 SSL 软件
Dependencies Resolved
========================================================================
 Package       Arch          Version                    Repository   Size
========================================================================
Installing:
 mod_ssl      x86_64      1:2.2.15-5.el6.centos          base         85 k
Transaction Summary
========================================================================
Install        1 Package(s)
Upgrade        0 Package(s)
```

```
Total download size: 85 k
Installed size: 183 k
```

## 配置SSL

首先编辑SSL配置文件，检查端口是否为443及前面是否有#号，另外LoadModule是指支持HTTP所需要的mod_ssl.so模块。

```
[root@localhost ~]# vi /etc/httpd/conf.d/ssl.conf         //编辑 SSL 配置文件
#
# This is the Apache server configuration file providing SSL support.
# It contains the configuration directives to instruct the server how to
# serve pages over an https connection. For detailing information about these
# directives see <URL:http://httpd.apache.org/docs/2.2/mod/mod_ssl.html>
#
# Do NOT simply read the instructions in here without understanding
# what they do.  They're here only as hints or reminders.  If you are unsure
# consult the online docs. You have been warned.
#
LoadModule ssl_module modules/mod_ssl.so                    //支持 SSL 模块
#
# When we also provide SSL we have to listen to the
# the HTTPS port in addition.
#
Listen 443                 //http ssl 默认端口为 443，如果有#号需删除才可以使用
```

## 配置防火墙

SSL服务必须在防火墙配置中开启443端口，HTTPS才可以对外连接。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT  //SSL 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                        [  OK  ]
```

```
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

一切配置完成后，必须重新启动apache服务，Apache配置才会生效。

```
[root@localhost ~]# service httpd restart
Stopping httpd:                                              [  OK  ]
Starting httpd:                                              [  OK  ]
```

## 测试Apache SSL是否正常运行

在浏览器中输入【https://IP或网址】如果出现如下图所示的页面，表示已正确加载mod_ssl模块，按【继续浏览此网站（不推荐）】，则进入网站，如果按【单击此处关闭该网页】，则关闭窗口。




> **说明**
>
> 数字证书请到数字证书中心申请。
>
> 如果不提供SSL服务，一定要删除mod_ssl，输入【yum remove mod_ssl】。

下面提供几个国内常见的数字证书管理中心。

| | |
|---|---|
| 北京数字证书管理中心 | http://www.bjca.org.cn/ |
| 上海数字证书管理中心 | http://www.sheca.com/default.aspx |
| 广州数字证书管理中心 | http://www.gzca.gd.cn/ |

# 5.8 配置Apache支持用户认证功能

在网站管理中，为了确保特定网页目录的访问安全性，需要配置Apache服务对该网页目录进行用户认证，就是登录这些网页目录时，需要输入用户名和密码，输入完成后才可以浏览网页。

## 开启Apache目录认证功能

如果让Apache支持目录认证功能，首先在配置文件中开启此功能，将AllowOverride None改成【All】，这样就启动目录认证功能，其次创建需要认证的目录。

```
[root@localhost /]# vi  /etc/httpd/conf/httpd.conf
# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
    AllowOverride All                          //默认为 None，修改为 All
…中间省略…

AccessFileName .htaccess                       //登录密码文件的存放位置
…中间省略…
<Directory "/var/www/html/security">           //创建认证目录
    AllowOverride AuthConfig                  //默认为 None，修改为 AuthConfig
    Order allow,deny
    Allow from all
</Directory>
```

配置完成后，必须重新启动Apache服务，配置才会生效。

```
[root@localhost /]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

## 创建认证用户密码

首先在/var/www/html目录下创建目录名称为security，此名称可以根据自己的需要命名，不一定要使用security，其次就是创建登录密码文件【.htpasswd】，示例中登录的用户名为jerry，用户可以自行配置，此用户与服务器用户无关系，要访问/var/www/html/security这个目录，创建登录密码文件时，会要求输入两次密码，用户密码创建成功后会有提示信息。

```
[root@localhost /]# mkdir /var/www/html/security      //创建认证目录
[root@localhost /]# htpasswd -c /var/www/html/security/.htpasswd jerry
                                                      //创建登录密码文件
New password:                                         //输入两次密码
Re-type new password:
Adding password for user jerry                        //创建登录密码文件成功
```

说明

认证目录security名称可以自行配置，一旦修改后请重新修改Apache配置文件及命令中指定的文件路径。

注意第一次新增用户时要加上-c，如果后续添加用户就不必加上-c，例如要新增用户ken，添加用户的命令是【htpasswd /var/www/html/security/.htpasswd ken】。

修改用户密码的命令是【htpasswd -m /var/www/html/security/.htpasswd jerry】，加上参数【-m】就可以修改。

首先检查/var/www/html/security目录下的【.htpasswd】是否成功创建。

```
[root@localhost security]# ls  -al /var/www/html/security //检查.htpasswd是否创建
total 16
drwxr-xr-x. 2 root root 4096 Aug 19 08:40 .
drwxr-xr-x. 3 root root 4096 Aug 19 08:35 ..
-rw-r--r--. 1 root root  103 Aug 19 08:40 .htaccess
-rw-r--r--. 1 root root   20 Aug 19 09:33 .htpasswd       //登录密码文件
```

其次检查.htpasswd配置文件的内容，示例中jerry为登录用户，密码经过加密，无法得知原始密码，如果忘记了密码，只能重新配置密码。

```
[root@localhost /]# cat /var/www/html/security/.htpasswd
jerry:QdTZSKwGloTL.
```

成功创建密码文件后，接下来就是在认证目录下配置.htaccess文件。

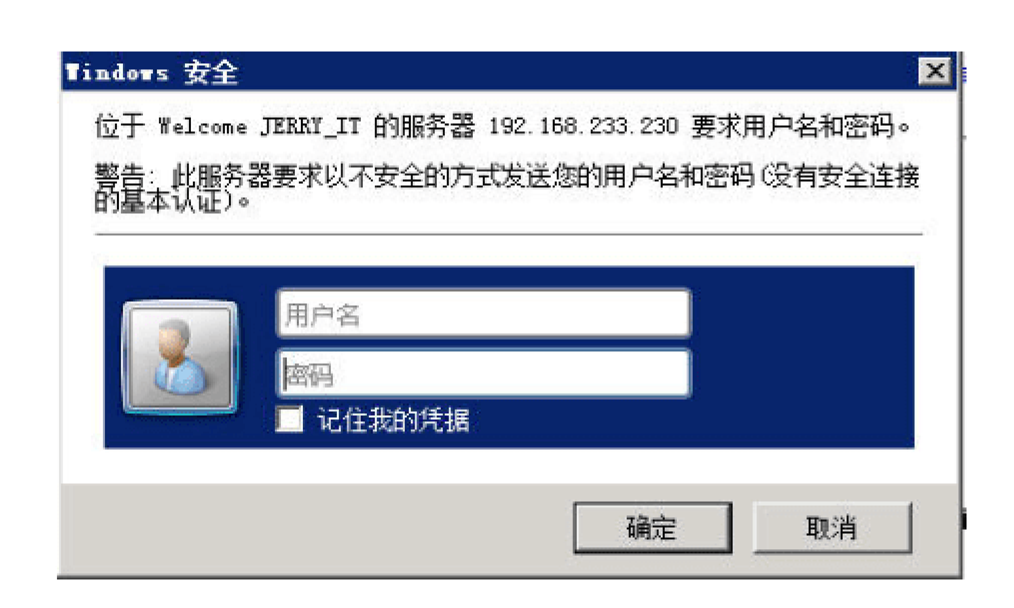
```
[root@localhost ~]# vi /var/www/html/security/.htaccess   //认证目录
AuthUserFile /var/www/html/security/.htpasswd
AuthName "Welcome Jerry_it"
AuthType Basic
require valid-user
```

说明

.htaccess文件是Apache服务器中的一个配置文件，一般情况下为默认文件，如果文件名不同，必须修改Apache配置文件，否则无法使用。

## 测试浏览目录是否需输入用户名和密码

配置完成后，在浏览器中输入【http://IP或网址/security】，浏览器会弹出登录窗口，如下图所示，请输入.htpasswd中创建的用户名和密码，示例中用户名为jerry，输入jerry用户的密码，输入完成后，按【确定】。




登录成功后，浏览器会转换至下图的画面。




连续3次错误输入密码后，浏览器会显示如下图所示的认证错误信息。




说明

如果输入用户名和密码后，一直出现登录界面，则是Apache配置文件忘记加上以下文字。

```
<Directory "/var/www/html/security">
   AllowOverride AuthConfig
    Order allow,deny
    Allow from all
</Directory>
```

## 5.9 配置Apache虚拟目录

如今很多网站上都有不同的应用系统，所以有的公司网站上可能有很多站点，有时候由于主机数量有限，在一台主机上可能需要挂载很多网站，Apache就是利用虚拟目录来配置多个网站，让多个网站同时存在于同一台网站服务器上。

## 环境介绍

现有一台网站服务器，有两个网站blog.jerryit.idv.cn和media.jerryit.idv.cn必须存在于同一台Web网站主机上，相关数据如下。

| 应用名称 | 服务器地址 | 类型 |
| --- | --- | --- |
| 网站服务器 | 192.168.1.98 | 主机（A） |
| blog | blog.jerryit.idv.cn | 别名（CNAME） |
| media | media.jerryit.idv.cn | 别名（CNAME） |

## 配置DNS

将以上数据配置到DNS服务器上，这里用Windows Server 2003作为DNS服务，读者可以自己根据需求配置，在DNS服务上添加Web网站服务器A的地址192.168.233.128，并配置两个别名（CNAME）记录为blog及media，两者同时指向Web网站服务器A，配置如下图所示。




## 创建blog和media网站目录

在/var/www/html目录下创建blog和media两个网站的目录。

```
[root@localhost /]# mkdir /var/www/html/blog             //创建 blog 目录
[root@localhost /]# mkdir /var/www/html/media            //创建 media 目录
```

> **说明**
>
> 如果网页目录路径配置不正确，请修改Apache的配置文件。

## 创建blog和media范例网页

在blog和media两个网站目录内创建范例网页。

```
[root@localhost /]# echo "Hello blog.jerryit.idv.cn" > /var/www/html/blog/index.html
[root@localhost /]# echo "Hello media.jerryit.idv.cn" > /var/www/html/media/index.html
```

> **说明**
> 可自行创建范例网页，也可以上传其他范例网页，上述两个范例网页是为了区分测试。

## 配置Apache网站虚拟目录

要创建网站虚拟目录，必须编辑Apache配置文件，将blog和media虚拟目录信息写入httpd.conf配置文件，Apache配置文件内有虚拟目录范例。

```
[root@localhost /]# vi /etc/httpd/conf/httpd.conf
#<VirtualHost *:80>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
```

将范例复制两份，将范例前面的#号删除，依次修改范例内容，输入内容如下所示。

```
[root@localhost /]# vi /etc/httpd/conf/httpd.conf
<VirtualHost  *:80>
    ServerAdmin admin@jerryit.idv.cn
    DocumentRoot /var/www/html/blog               //网页主目录
    ServerName blog.jerryit.idv.cn                //网址名称
    ErrorLog logs/blog.jerryit.idv.cn-err_log
    CustomLog logs/blog.jerryit.idv.cn-access_log common
</VirtualHost>

<VirtualHost  *:80>
    ServerAdmin admin@jerryit.idv.cn
    DocumentRoot /var/www/html/media              //网页主目录
    ServerName media.jerryit.idv.cn               //网址名称
    ErrorLog logs/media.jerryit.idv.cn-err_log
    CustomLog logs/media.jerryit.idv.cn-access_log common
</VirtualHost>
```

| Apache 虚拟目录配置文件说明 | |
| --- | --- |
| **参数** | **说明** |
| NameVirtualHost | 虚拟主机 IP 地址，例如 192.168.233.128 |
| VirtualHost | 网站 IP 及端口，例如 192.168.233.128:80 |
| ServerAdmin | 网站管理员 E-Mail，例如 admin@jerryit.idv.cn |

（续表）

| 参数 | 说明 |
| --- | --- |
| DocumentRoot | 网站存放日志目录，例如/var/www/html/blog |
| ServerName | 网站网址，例如 blog.jerryit.idv.cn |
| ErrorLog | 错误日志文件，位置在/var/log，例如 blog.jerryit.idv.cn-err_log |
| CustomLog | 访问日志文件，例如 blog.jerryit.idv.cn-access_log |

确认NameVirtualHost端口为80。

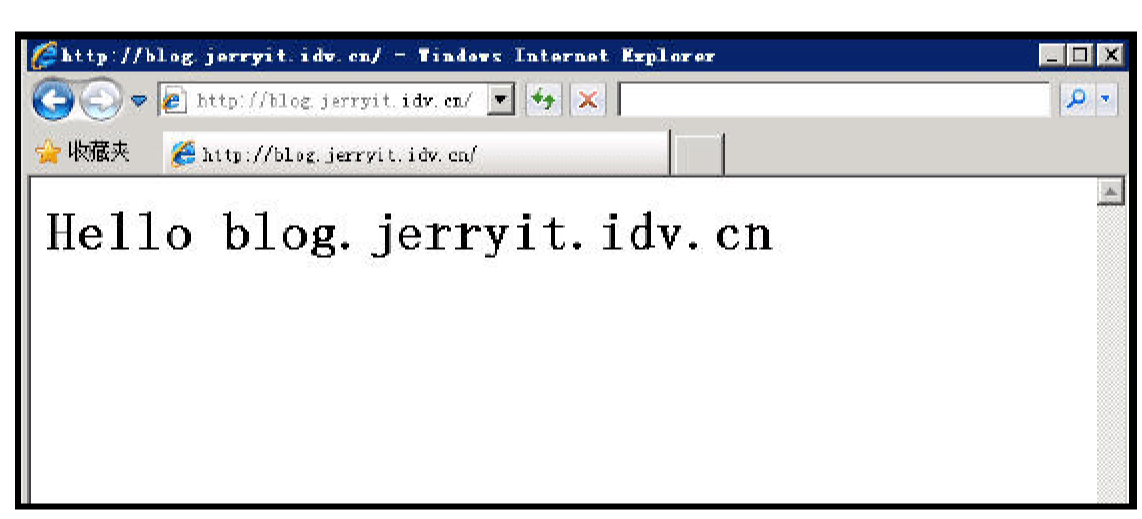
```
[root@localhost /]# vi /etc/httpd/conf/httpd.conf
# Use name-based virtual hosting.
#
NameVirtualHost *:80
#
```

如果不是80端口，修改配置完成后，必须重新启动Apache服务，配置才会生效。

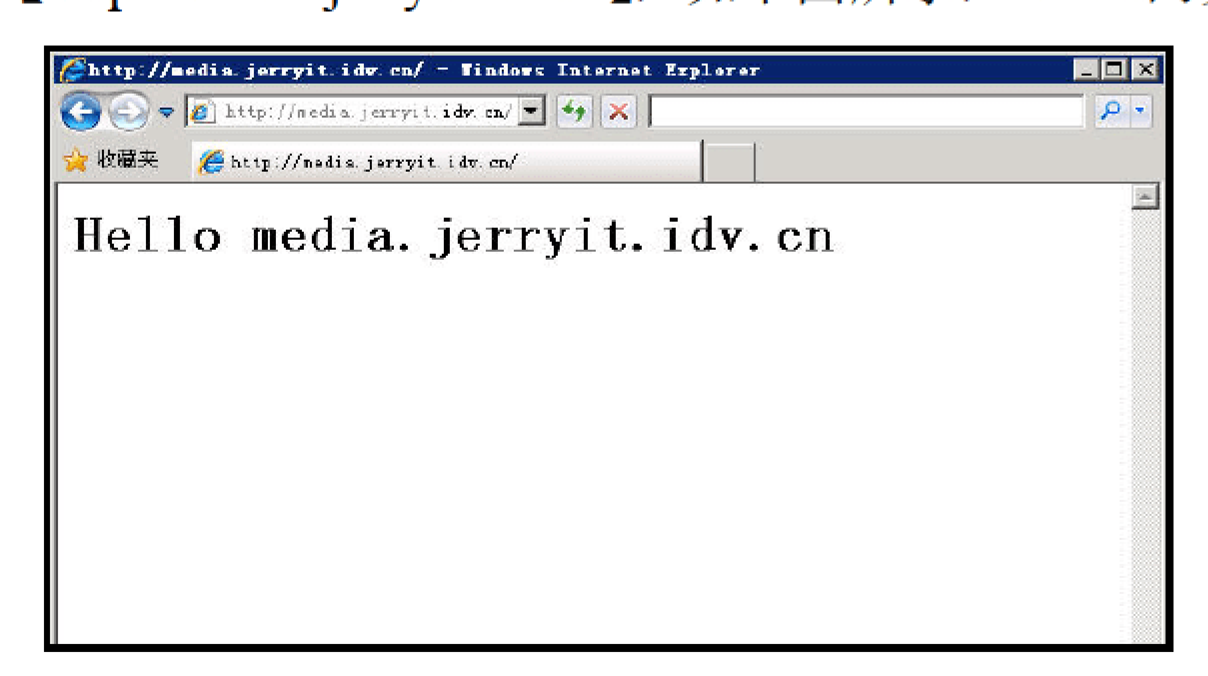
```
[root@localhost /]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

## 测试Apache虚拟目录

打开浏览器，输入【http://blog.jerryit.idv.cn】，如下图所示，blog网页可以正常开启。




在浏览器中输入【http://media.jerryit.idv.cn】，如下图所示，media网页可以正常开启。




如果blog.jerryit.idv.cn和media.jerryit.idv.cn可以正常浏览，代表虚拟目录及DNS配置成功，如果需配置第三个虚拟目录，可以依此类推。

## 配置虚拟目录后网页无法浏览

步骤01 使用nslookup命令查询两个范例的网站，如果不能正确查询，需检查DNS的CNAME记录是否配置正确。

步骤02 如果DNS可以正常查询，网站还是无法浏览，需要检查httpd.conf配置文件的虚拟目录配置是否正确或修改httpd.conf配置文件后，Apache是否重新启动。

步骤03 检查浏览器是否使用proxy，如果使用proxy，将其取消，再测试查看网页是否可以正常浏览。

# 第6章

# Tomcat——网站服务器

Tomcat官方网站：http://tomcat.apache.org/。

Tomcat是Apache软件基金会下属的Jakarta项目中的一个核心项目，由Sun Microsystems提供技术规范，实现了对Servlet和JavaServer Page（JSP）的支持，并提供了Web服务器的一些特有功能，如增强了服务器管理程序和服务器管理程序的安全性等。由于Tomcat本身是HTTP服务器的扩展，它也可以被当作一个单独的Web服务器使用。但是，不能将Tomcat和Apache服务器混淆，因为Apache Server是一个用C语言实现的HTTP Web Server；这两个HTTP Web Server软件不是捆绑在一起的。Tomcat包含一个配置管理工具，也可以通过编辑XML格式的配置文件来进行配置。

## 6.1 配置Tomcat 6环境

Tomcat 6实现了对Servlet 2.5和JSP 2.1等特性的支持，CentOS操作系统目前无法使用Yum在线更新方式安装，所以必须到官方网站下载软件安装。

Tomcat 6软件下载网站：http://tomcat.apache.org/download-60.cgi。

Tomcat 6.0.35版本下载地址：http://mirrors.tuna.tsinghua.edu.cn/apache/tomcat/tomcat-6/v6.0.35/bin/apache-tomcat-6.0.35.tar.gz。

### 检查JDK软件

检查是否已安装JDK软件，CentOS 6.x默认已安装，若要安装其他版本，请到Oracle官网下载。

```
[root@localhost ~]# rpm -qa | grep jdk
java-1.6.0-openjdk-1.6.0.0-1.21.b17.el6.x86_64
```

> **说明**
>
> JDK 6下载地址
>
> http://www.oracle.com/technetwork/java/javase/downloads/jdk-6u27-download-440405.html

## 安装Tomcat 6

使用wget下载方式将Tomcat6压缩文件下载到/usr/local目录下，解压缩后，将目录名称重命名为tomcat6。

```
[root@localhost ~]# cd /usr/local                    //进入/usr/local 目录
[root@localhostlocal]#wget
http://mirrors.tuna.tsinghua.edu.cn/apache/tomcat/tomcat-6/v6.0.35/bin/apache-tomcat-6
.0.35.tar.gz  …中间省略…
[root@localhost local]# tar -zxvf apache-tomcat-*.tar.gz   //解压缩
…中间省略…
[root@localhost local]# mv apache-tomcat-6.0.35 tomcat6   //重命名 tomcat 目录名称
```

> **说明**
>
> Tomcat最新版本按照官网公布为准。

## 启动及关闭Tomcat 6

进入Tomcat6的bin目录，启动Tomcat 6。

```
[root@localhost local]#  cd tomcat6/bin          //进入 tomcat6 的 bin 目录
[root@localhost bin]# ./startup.sh               //启动 tomcat6
Using CATALINA_BASE:     /usr/local/tomcat6
Using CATALINA_HOME:     /usr/local/tomcat6
Using CATALINA_TMPDIR:   /usr/local/tomcat6/temp
Using JRE_HOME:          /usr
Using CLASSPATH:         /usr/local/tomcat6/bin/bootstrap.jar
```

Tomcat服务启动与关闭的方式如下表所示。

| | |
|---|---|
| **启动 Tomcat 6** | /usr/local/tomcat6/bin/startup.sh |
| **关闭 Tomcat 6** | /usr/local/tomcat6/bin/shutdown.sh |

## Tomcat目录说明

Tomcat相关目录如下表所示，路径与Apache相似。

| | |
|---|---|
| **网页存放目录** | /usr/local/tomcat6/webapps/ROOT |
| **日志文件目录** | /usr/local/tomcat6/logs |
| **配置文件目录** | /usr/local/tomcat6/conf |

## 配置防火墙

Tomcat 6默认端口为8080，必须在防火墙配置中开启8080端口才可以对外连接。

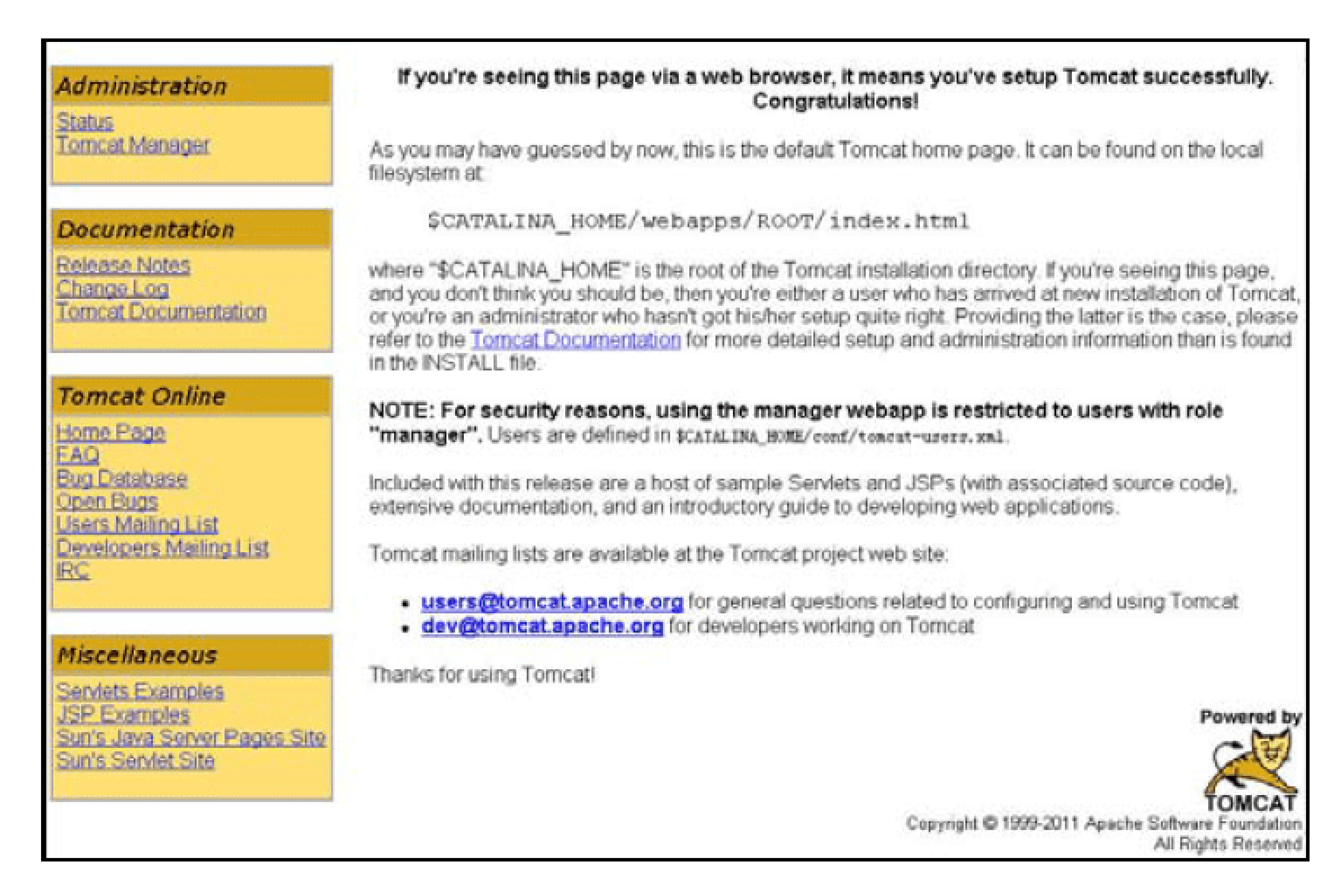
```
[root@localhost local]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
                                                          //tomcat 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动服务，配置才会生效。

```
[root@localhost local]# service iptables restart
iptables: Flushing firewall rules:                        [  OK  ]
iptables: Setting chains to policy ACCEPT: filter         [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

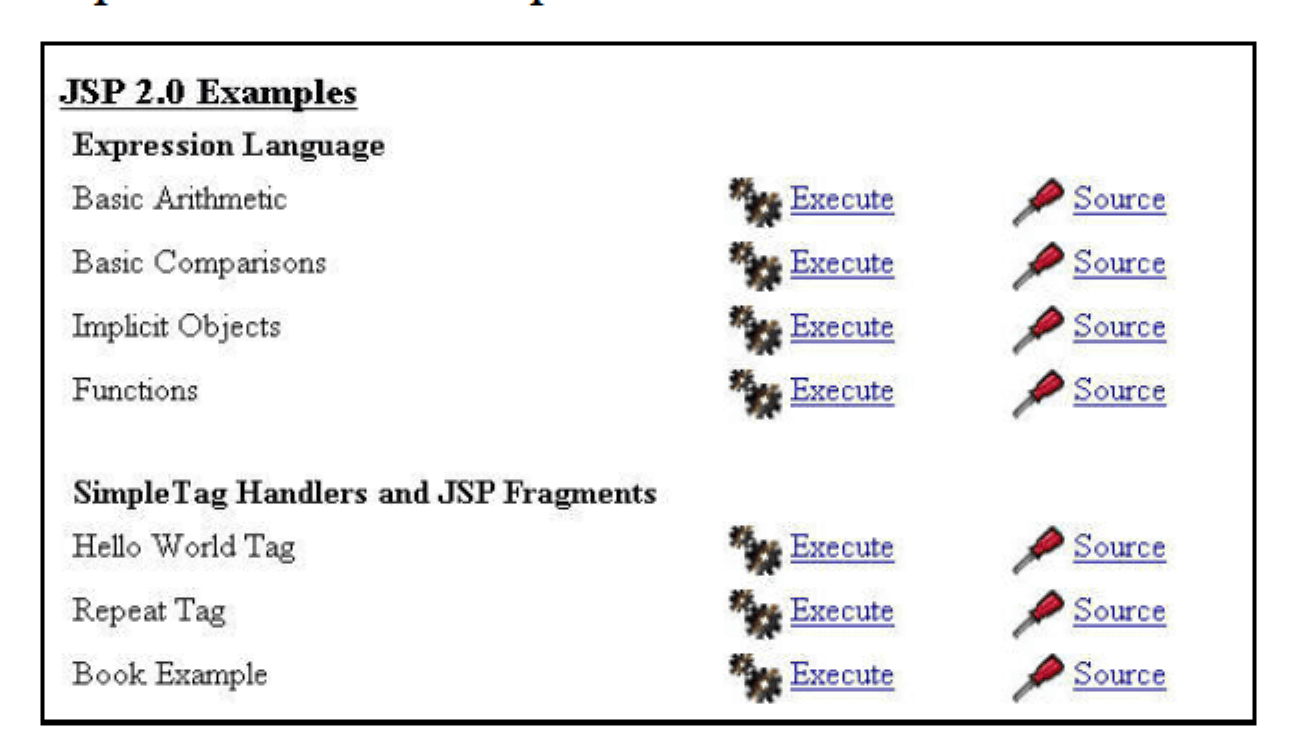
## 测试Tomcat 6是否运行正常

在浏览器中输入【http://IP地址:8080】，默认Tomcat 6端口为8080，下图所示表示Tomcat 6安装成功。



> **说明**
>
> 输入网址或IP地址时要加上http，否则会无法识别。

分别测试JSP Examples和Servlet Examples示例网页是否可以正常浏览。




## 6.2 配置Tomcat 7环境

Tomcat 7实现了对于Servlet 3.0、JSP 2.2和EL 2.2等特性的支持，提高了服务器的安全性，降低了遭受攻击的可能。

Tomcat 7软件下载网站：http://tomcat.apache.org/download-70.cgi。

Tomcat 7.0.29版本下载地址：http://mirror.bit.edu.cn/apache/tomcat/tomcat-7/v7.0.29/bin/apache-tomcat-7.0.29.tar.gz。

最新版本依官方网站为准。

### 检查JDK软件

检查是否已安装JDK，CentOS 6.x默认已安装，若要安装其他版本，请到Oracle官网下载。

```
[root@localhost ~]# rpm -qa | grep jdk
java-1.6.0-openjdk-1.6.0.0-1.21.b17.el6.x86_64
```

> **说明**
>
> JDK 7下载地址：http://www.oracle.com/technetwork/java/javase/downloads/java-se-jdk-7-download-432154.html。

### 安装Tomcat 7软件

使用wget下载方式将压缩文件下载到/usr/local目录下，解压缩后，将目录重命名为tomcat7。

```
[root@localhost ~]# cd /usr/local    //进入/usr/local 目录
[root@localhost local]# wget
http://mirror.bit.edu.cn/apache/tomcat/tomcat-7/v7.0.29/bin/apache-tomcat-7.0.29.tar.g
z
…中间省略…
[root@localhost local]# tar -zxvf  apache-tomcat-7.0.29.tar.gz   //解压缩文件
…中间省略…
[root@localhost local]# mv apache-tomcat-7.0.29 tomcat7 //将目录重命名为 tomcat7
```

## 启动Tomcat 7

要启动Tomcat 7，需要进入Tomcat的bin目录，该目录下的命令用于管理Tomcat服务。

```
[root@localhost local]#   cd tomcat7/bin       //进入 Tomcat  7 的 bin 目录
[root@localhost bin]#  ./startup.sh            //启动 Tomcat7
Using CATALINA_BASE:      /usr/local/tomcat7
Using CATALINA_HOME:      /usr/local/tomcat7
Using CATALINA_TMPDIR:    /usr/local/tomcat7/temp
Using JRE_HOME:           /usr
Using CLASSPATH:
/usr/local/tomcat7/bin/bootstrap.jar:/usr/local/tomcat7/bin/tomcat-juli.jar
```

Tomcat服务的启动与关闭方法如下表所示。

| | |
|---|---|
| 启动 Tomcat 7 | /usr/local/tomcat7/bin/startup.sh |
| 关闭 Tomcat 7 | /usr/local/tomcat7/bin/shutdown.sh |

## 防火墙设定

Tomcat 7默认端口为8080，所以必须在防火墙配置中开启8080端口才可以对外连接。

```
[root@localhost /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
                                                           //tomcat 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

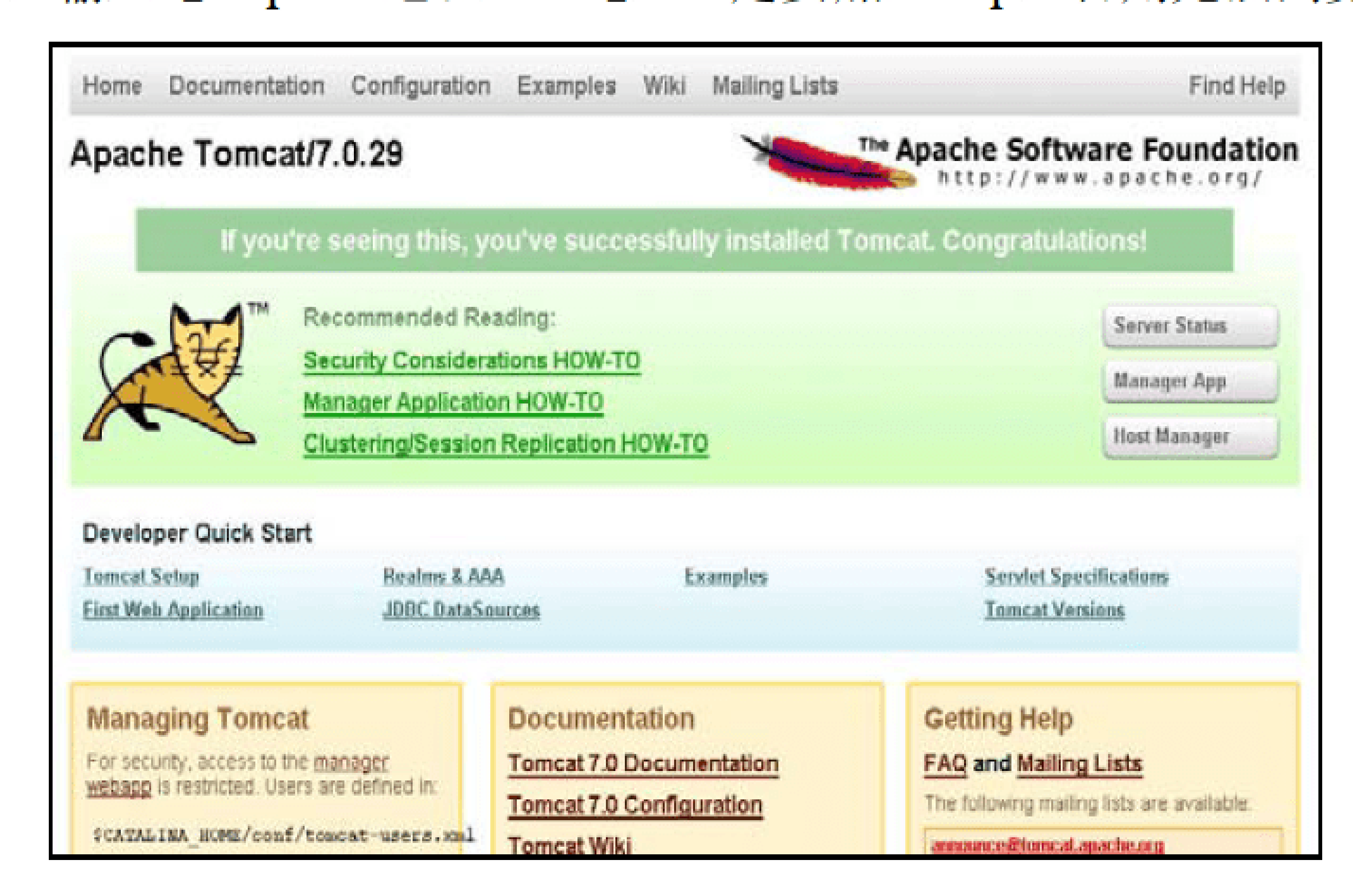
防火墙配置完成后，必须重新启动服务，配置才会生效。

```
[root@localhost /]# service iptables restart
iptables: Flushing firewall rules:                      [  OK  ]
```

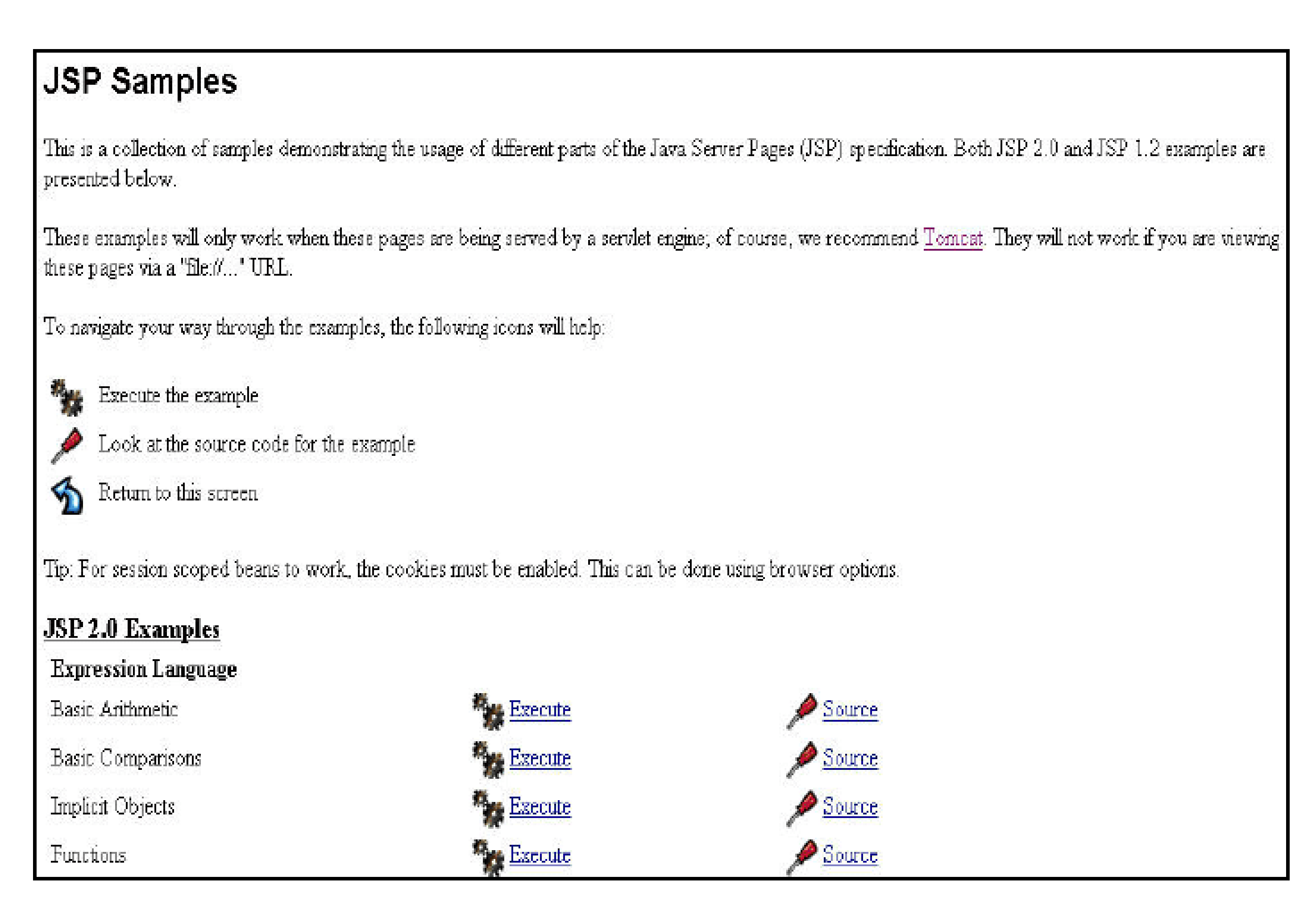
```
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

## 测试Tomcat 7是否正常运作

打开浏览器，输入【http://IP地址:8080】，一定要加上http，否则无法浏览Tomcat 7首页。




测试示例网页是否可以浏览，输入【http://IP:8080/examples/jsp/】，选择其中一个Execute即可测试。



# 第7章

# MySQL——数据库

MySQL官方网站：http://www.mysql.com/。

MySQL由于性能高、成本低、可靠性好，已经成为现今最流行的开源数据库，被广泛地应用在中小型网站中。随着MySQL的不断成熟，它也逐渐用于更多大规模网站，比如维基百科、Google和Facebook。非常流行的开源软件组合LAMP中的M就是指MySQL。

## 系统特性

- 使用C和C++编写，并使用了多种编译程序进行测试，保证源代码的可移植性。
- 支持AIX、BSDi、FreeBSD、HP-UX、Linux、Mac OS、Novell NetWare、NetBSD、OpenBSD、OS/2 Wrap、Solaris、Windows等多种操作系统。
- 为多种编程语言提供了API。这些编程语言包括C、C++、C#、VB.NET、Delphi、Eiffel、Java、Perl、PHP、Python、Ruby和Tcl等。
- 支持多线程，充分利用CPU资源，支持多用户。
- 优化的SQL查询算法，有效地提高查询速度。
- 既能够作为一个单独的应用程序应用在客户端服务器网络环境中，也能够作为一个库嵌入到其他的软件中。
- 提供多语言支持，常见的编码如中文的GB2312/BIG5、日文的Shift_JIS等都可以用作数据表名和数据列名。
- 提供TCP/IP、ODBC和JDBC等多种数据库连接途径。
- 提供用于管理、检查、优化数据库操作的管理工具。
- 可以处理拥有上千万条记录的大型数据库。

## 7.1 安装MySQL数据库

本章介绍该如何安装MySQL数据库，安装完成后如何配置环境及相应的操作。

## 检查MySQL数据库是否安装

安装前先检查是否已安装MySQL数据库，有些版本在安装操作系统时已经安装。

```
[root@localhost ~]# rpm -qa|grep mysql      //检查 MySQL 软件
mysql-server-5.1.52-1.el6_0.1.x86_64
mysql-libs-5.1.52-1.el6_0.1.x86_64
mysql-5.1.52-1.el6_0.1.x86_64
```

## 安装MySQL数据库

安装MySQL数据库软件，基本上需要安装mysql及mysql-server这两个软件。

```
[root@localhost ~]# yum install -y mysql mysql-server
Dependencies Resolved
========================================================================
 Package     Arch      Version     Repository  Size
========================================================================
Installing:
 mysql              x86_64   5.1.52-1.el6_0.1     updates     889 k
 mysql-server       x86_64   5.1.52-1.el6_0.1     updates     8.1 M
Installing for dependencies:
 perl-DBD-MySQL     x86_64   4.013-3.el6          base        134 k
Updating for dependencies:
 mysql-libs         x86_64   5.1.52-1.el6_0.1     updates     1.2 M
Transaction Summary
========================================================================
Install       3 Package(s)
Upgrade       1 Package(s)
Total download size: 10 M
```

## MySQL的启动和关闭

安装MySQL数据库完毕后，第一次启动MySQL数据库时，除了欢迎信息，还会提醒必须要配置MySQL数据库密码，MySQL数据库默认无密码，配置密码较为安全。

```
[root@localhost ~]# service mysqld start     //启动 MySQL
Initializing MySQL database:  Installing MySQL system tables...
OK
Filling help tables...
OK
To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system
PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:
/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h localhost.localdomain password 'new-password'
```

```
Alternatively you can run:
/usr/bin/mysql_secure_installation
which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
See the manual for more instructions.
You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &
You can test the MySQL daemon with mysql-test-run.pl
cd /usr/mysql-test ; perl mysql-test-run.pl
Please report any problems with the /usr/bin/mysqlbug script!
                                                            [  OK  ]
Starting mysqld:                                            [  OK  ]
```

MySQL数据库每次开机都要运行，因此必须将MySQL数据库配置为系统默认启动，输入【chkconfig mysqld on】，这样MySQL数据库在系统重新启动后也会自动启动。下表列出了经常使用的MySQL数据库状态管理命令。

| 说明 | 命令 |
|---|---|
| 启动数据库 | service mysqld start |
| 关闭数据库 | service mysqld stop |
| 重新启动数据库 | service mysqld restart |
| 查看数据库运行状态 | service mysqld status |

## MySQL的登录和退出

MySQL数据库分为有密码及无密码的登录，默认安装好后，MySQL数据库没有密码，所以不用加上参数P，若配置密码后，则要加上参数P才可以登录，以下是两种登录方法，退出的方法为输入quit或exit。

```
---------------------------默认无密码方式登录-----------------------------
[root@localhost ~]# mysql -u root    //默认无密码登录
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.1.52 Source distribution
Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> quit          //退出 MySQL
Bye

-------------------------有密码方式登录----------------------------------
[root@localhost ~]# mysql -u root -p
Enter password:
```

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.1.52 Source distribution
Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> exit
Bye
[root@localhost ~]#
```

## 配置MySQL数据库密码

第一次启动MySQL数据库时是没有密码的，所以要配置密码，可确保MySQL数据库的安全性，配置密码方法说明如下，默认都会配置root用户账号的密码。

```
mysqladmin  -u 用户  password  密码
```

下面介绍如何配置MySQL数据库的密码，就以root账号为例来配置MySQL数据库密码，首先检查MySQL数据库是否为启动状态，否则无法配置密码。

```
[root@localhost ~]# service mysqld status                //检查 MySQL 状态
mysqld (pid  9113) is running...
[root@localhost ~]# mysqladmin -u root password Aa1234567       //配置密码
```

若没有启动MySQL数据库，配置密码时会出现错误信息。

```
[root@localhost ~]# mysqladmin -u root password Aa1234567
mysqladmin: connect to server at 'localhost' failed
error: 'Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock'
(2) '
Check that mysqld is running and that the socket: '/var/lib/mysql/mysql.sock' exists!
```

## 修改数据库用户密码

MySQL数据库配置好密码后，也有可能需要修改密码，修改密码的方法如下，需要输入旧密码，若没有旧密码则无法修改。

```
mysqladmin  -u 用户  -p password  新密码
```

用刚刚配置好的root用户来修改密码。

```
[root@localhost ~]# mysqladmin -u root -p password Aa12345678 //变更密码
Enter password:                                               //输入旧密码
[root@localhost ~]#
```

## 重设root密码

若忘记MySQL数据库的root用户密码，就无法登录使用，必须想办法重新配置密码。下面介绍重设用户密码的方法，首先将MySQL数据库关闭，其次以--skip-grant-table 的参数启动MySQL数据库。以下步骤较多，请勿遗漏，修改完密码后，测试是否可以以新密码登录。

```
[root@localhost ~]# service mysqld stop            //关闭 MySQL
Stopping mysqld:                                           [  OK  ]
[root@localhost ~]# /usr/bin/mysqld_safe --skip-grant-table &
          //进入 MySQL 安全模式，通常会卡住，其实是在后台运行，所以一分钟后按 Ctrl+C
[1] 3237
[root@localhost ~]# 110901 09:50:09 mysqld_safe Logging to '/var/log/mysqld.log'.
110901 09:50:09 mysqld_safe Starting mysqld daemon with databases from /var/lib/mysql
[root@localhost ~]# mysql -u root                  //无密码方式登录
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1
Server version: 5.1.52 Source distribution
Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> use mysql;                                 //使用 MySQL 数据库
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> update user set password=PASSWORD("Aa1234567") where User='root';
Query OK, 3 rows affected (0.00 sec)
Rows matched: 3  Changed: 3  Warnings: 0
                              //配置 Aa1234567 为新密码，root 为被修改的账号
mysql> flush privileges;                          //更新写入
Query OK, 0 rows affected (0.00 sec)
mysql> quit                                       //修改密码完成，退出 MySQL 数据库
Bye
[root@localhost ~]# service mysqld restart        //重新启动 MySQL，取消安全模式登录
110901 09:54:44 mysqld_safe mysqld from pid file /var/run/mysqld/mysqld.pid ended
Stopping mysqld:                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
[1]+  Done                   /usr/bin/mysqld_safe --skip-grant-table
[root@localhost ~]# mysql -u root -p              //使用密码方式登录
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.1.52 Source distribution
Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
mysql> quit                                      //可以用修改后的密码登录，确认后退出
Bye
[root@localhost ~]#
```

## 创建、删除、查看数据库

系统管理员最常用到的MySQL数据库操作就是查看、创建、删除，如果想执行更详细的操作，请使用MySQL数据库管理软件来管理操作，如使用phpMyAdmin或navicat。下面以DB1为范例数据库来进行介绍。

```
[root@localhost ~]# mysql -u root -p                //以密码方式登录 MySQL
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.1.52 Source distribution
Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> create database db1;                         //创建 DB1 数据库
Query OK, 1 row affected (0.00 sec)
mysql> show databases;                              //查看 MySQL 所有数据库
+-------------------------+
| Database                |
+-------------------------+
| information_schema      |
| db1                     |
| mysql                   |
| test                    |
+-------------------------+
4 rows in set (0.00 sec)
mysql> drop database db1;                           //删除 DB1 数据库
Query OK, 0 rows affected (0.01 sec)
mysql> quit                                         //退出 MySQL
Bye
```

说明

范例数据库名称为DB1。

## MySQL配置文件内容说明

了解了一些管理MySQL数据库的方式和配置，也要了解MySQL数据库配置文件的内容，即数据库的存放路径及日志文件的路径，以便日后进行配置及备份。

```
[root@localhost ~]# vi /etc/my.cnf        // /etc/my.cnf 为 MySQL 配置文件的位置
```

```
[mysqld]
datadir=/var/lib/mysql                  //数据库文件目录
socket=/var/lib/mysql/mysql.sock        // Socket 文件
user=mysql
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
[mysqld_safe]
log-error=/var/log/mysqld.log           //数据库日志文件
pid-file=/var/run/mysqld/mysqld.pid     //进程 PID 文件
```

## 7.2 修改MySQL数据库端口

每个数据库的运行都会用到端口，Microsoft SQL Server端口为1433，MySQL数据库默认端口为3306，通常不会修改数据库的端口，因为修改数据库端口会有安全性问题，如果有端口冲突现象，才需要修改，首先不考虑什么原因，如何修改端口还是需要知道的，修改前先检查数据库使用的端口。

```
[root@localhost ~]# netstat  -tunlp | grep mysqld
tcp     0  0 0.0.0.0:3306            0.0.0.0:*              LISTEN   3476/mysqld
```

如果要修改MySQL数据库端口，必须在MySQL数据库配置文件中修改，默认里面没有配置端口的参数，MySQL数据库默认端口就是3306，所以要使用其他的端口就必须自行修改，例如，要将端口修改成3305，就需要在【mysqld】配置项的最后一行加上端口参数与所要使用的端口号，配置完成后，保存退出。

```
[root@localhost ~]# vi /etc/my.cnf                    //编辑 MySQL 配置文件
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
port=3305                                      //默认没有此行，配置端口为 3305

[mysqld_safe]
log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

修改MySQL数据库端口后，必须重新启动MySQL数据库服务，MySQL配置才会生效。

```
[root@localhost ~]# service mysqld restart
Stopping mysqld:                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

说明

记得将防火墙的端口改成3305，否则无法使用。

如果重新启动发生错误，问题就出在SELinux的安全性上，建议将SELinux关闭。

```
[root@localhost ~]# service mysqld restart
Stopping mysqld:                                           [  OK  ]
MySQL Daemon failed to start.
Starting mysqld:                                           [FAILED]
```

重新启动MySQL数据库后，检查MySQL数据库是否以端口3305运行，如果是的话表示修改成功，如果不是的话，重新检查配置文件，确定错误位置并修改。

```
[root@localhost ~]# netstat  -tunlp | grep mysqld
tcp        0      0 0.0.0.0:3305            0.0.0.0:*               LISTEN1838/mysqld
```

# 7.3 MySQL数据库权限配置

MySQL数据库用户权限的授权或删除分为本机登录及远程登录，因为MySQL数据库权限配置会将账号的权限配置给指定主机，如果配置为localhost，那该账号只能在MySQL数据库本机使用，如果要开放远程主机连接MySQL数据库，那就必须将账号配置给远程主机使用，下面介绍的方法都是授权或删除所有权限，MySQL的权限有很多，可以参考下表。

| 数据库（DateBase）十五种权限 |
|---|
| ALL PRIVILEGES、ALTER、CREATE、DELETE、DROP、FILE、INDEX、INSERT、PROCESS、REFERENCES、RELOAD、SELECT、SHUTDOWN、UPDATE、USAGE |

| 数据表（Table）八种权限 |
|---|
| SELECT、INSERT、UPDATE、DELETE、CREATE、DROP、INDEX、ALTER |

| 数据域（column）三种权限 |
|---|
| SELECT INSERT UPDATE |

## 授权用户权限

假如授权用户账号jerry有本机及远程管理的权限，那么需要在MySQL数据库中配置允许远程登录的IP地址，首先配置jerry允许远程登录的IP为192.168.233.2，假如使用192.168.233.3的IP地址就不能远程登录，其次再配置允许远程连接IP地址的远程管理权限。下面示范如何授权本机管理权限及远程管理权限。

| MySQL 数据库用户权限命令说明 | |
|---|---|
| Grant | 授权 |
| all privileges | 所有管理权限 |
| *.* | 所有数据库 |
| Localhost | 本机地址 |

（续表）

| MySQL 数据库用户权限命令说明 | |
|---|---|
| 192.168.233.2 | 远程连接 IP 地址 |
| jerry | 授权账号 |
| Aa1234567 | 授权密码 |

管理权限的范例是所有权限，可根据实际情况按需求配置。

```
[root@localhost ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.1.52 Source distribution

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> grant all privileges on *.* to jerry@localhost identified by 'Aa1234567';
Query OK, 0 rows affected (0.00 sec)                //创建 jerry 本机管理权限

mysql> grant all privileges on *.* to jerry@192.168.233.2 identified by 'Aa1234567';
Query OK, 0 rows affected (0.01 sec)                //创建 jerry 账号远程管理


mysql> select host,user from mysql.user;            //查看 MySQL 所有授权账号
+-----------------------+-------+
| host                  | user  |
+-----------------------+-------+
| 127.0.0.1             | root  |
| 192.168.233.2         | jerry |                   //jerry 用户远程管理授权
| localhost             |       |
| localhost             | jerry |                   //jerry 用户本机管理授权
| localhost             | root  |
| localhost.localdomain |       |
| localhost.localdomain | root  |
+-----------------------+-------+
7 rows in set (0.00 sec)

mysql> quit                                        //退出 MySQL
Bye
[root@localhost ~]#
```

## 查看用户权限

不是每个用户都拥有所有的管理权限，如何得知目前登录的用户权限呢？以下示例说明如何查看jerry用户的权限，及目前登录用户的权限。

```
[root@localhost ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.1.52 Source distribution

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free
software,and you are welcome to modify and redistribute it under the GPL
v2 license

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW GRANTS FOR jerry@localhost;        //查看 jerry 用户本地权限
也可以输入 IP 地址
+------------------------------------------------------------------------
| Grants for jerry@localhost                                             |
+------------------------------------------------------------------------
| GRANT ALL PRIVILEGES ON *.* TO 'jerry'@'localhost'                    |
| IDENTIFIED BY PASSWORD '*5AF7F0C8FBF51E7D12F5BFBB4A39032C91A          |
| 10106'                                                                 |
+------------------------------------------------------------------------+
1 row in set (0.00 sec)

mysql> SHOW GRANTS;                     //查看当前登录用户权限，目前只有 root 登录
+------------------------------------------------------------------------
| Grants for root@localhost                                              |
+------------------------------------------------------------------------
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost'                     |
| IDENTIFIED BY PASSWORD '*5AF7F0C8FBF51E7D12F5BFBB4A39032C91A          |
| 10106' WITH GRANT OPTION                                               |
+------------------------------------------------------------------------+
1 row in set (0.00 sec)
mysql> quit                                                   //退出 MySQL
Bye
[root@localhost ~]#
```

## 删除用户及用户所有权限

当用户离职或不使用MySQL数据库后，就必须将该账号删除，以免增加MySQL数据库的风险，以下示范如何删除用户及该用户权限。

| MySQL 数据库授权用户权限指令说明 | |
|---|---|
| Revoke | 删除 |
| all privileges | 所有管理权限 |
| *.* | 所有数据库 |

（续表）

| MySQL 数据库授权用户权限指令说明 | |
|---|---|
| Localhost | 本机 |
| 192.168.233.2 | 远程主机 IP 地址 |
| jerry | 授权用户 |

管理权限的范例是所有权限，可根据实际情况配置。

```
……………………….MySQL 数据库权限……………………………
[root@localhost ~]# mysql -u root -p     //登录 MySQL
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.1.52 Source distribution

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> revoke all privileges on *.* from jerry@localhost;
Query OK, 0 rows affected (0.00 sec)  //删除 jerry 用户本机权限
mysql> revoke all privileges on *.* from jerry@192.168.233.2;
Query OK, 0 rows affected (0.00 sec)  //删除 jerry 用户远程登录权限
……….……………删除 MySQL 数据库账号…….…………………
mysql> use mysql;                //使用 MySQL
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> delete from user where user='jerry';//删除 jerry 用户
Query OK, 2 rows affected (0.00 sec)

mysql> flush privileges;                     //刷新数据库
Query OK, 0 rows affected (0.01 sec)

mysql> select host,user from mysql.user;    //检查用户是否还存在
+-----------------------+------+
| host                  | user |
+-----------------------+------+
| 127.0.0.1             | root |
| localhost             |      |
| localhost             | root |
| localhost.localdomain |      |
| localhost.localdomain | root |
+-----------------------+------+
5 rows in set (0.00 sec)
mysql> quit                                  //退出 MySQL
Bye
```

```
[root@localhost ~]#
```

# 7.4 phpMyAdmin管理工具

phpMyAdmin官方网站：http://www.phpmyadmin.net/home_page/index.php。

phpMyAdmin 是用PHP编写的，可以通过Web控制和操作MySQL数据库。通过phpMyAdmin可以完全对数据库进行操作，如创建、复制、删除数据库等。

## 安装phpMyAdmin软件

phpMyAdmin是由PHP写成的软件，所以需要用到PHP软件，其中php-mysql软件是为了让PHP可以连接到MySQL，除了PHP软件外，由于phpMyAdmin使用Web方式管理，所以也要安装Apache服务器。

```
[root@localhost ~]# yum install -y httpd  php  php-mysql  php-mbstring
Dependencies Resolved
=========================================================================
 PackageArch     Version        Repository  Size
=========================================================================
Installing:
 Httpd         x86_64      2.2.15-5.el6.centos base     811 k
 Php        x86_64      5.3.2-6.el6_0.1      updates  1.1 M
 php-mbstring x86_64      5.3.2-6.el6_0.1      updates  504 k
 php-mysql     x86_64      5.3.2-6.el6_0.1      updates  75 k
Installing for dependencies:
 Apr        x86_64      1.3.9-3.el6_0.1      updates  124 k
 apr-util      x86_64      1.3.9-3.el6_0.1      updates  87 k
 apr-util-ldap    x86_64      1.3.9-3.el6_0.1      updates15 k
 httpd-tools      x86_64      2.2.15-5.el6.centos base   68 k
 php-cli    x86_64      5.3.2-6.el6_0.1      updates  2.2 M
 php-common    x86_64      5.3.2-6.el6_0.1      updates  516 k
 php-pdo    x86_64      5.3.2-6.el6_0.1      updates  72 k
Transaction Summary
=========================================================================
Install    11 Package(s)
Upgrade    0 Package(s)
Total download size:   5.5 M
```

## 安装phpMyAdmin

使用wget命令下载phpMyAdmin压缩文件，下载后将phpMyAdmin压缩文件解压缩，phpMyAdmin是以Web方式管理的，所以要把解压缩后的phpMyAdmin目录拷贝到Apache网页主目录下，拷贝中顺便将目录名称改成phpMyAdmin，然后进入phpMyAdmin目录，复制模板

配置文件config.sample.inc.php并重命名为config.inc.php。

```
[root@localhost ~]# wget
http://sourceforge.net/projects/phpmyadmin/files/phpMyAdmin/3.5.2.2/phpMyAdmin-3.5.2.2
-all-languages.tar.gz           //下载 phpMyAdmin 压缩文件
[root@localhost ~]# tar -zxvf phpMyAdmin-3.5.2.2-all-languages.tar.gz
                                                     //解压缩
[root@localhost ~]# mv phpMyAdmin-3.5.2.2-all-languages
/var/www/html/phpMyAdmin                             //拷贝并重命名
[root@localhost ~]# cd  /var/www/html/phpMyAdmin
                                                     //进入 phpMyAdmin 目录
[root@localhost phpMyAdmin]# cp config.sample.inc.php config.inc.php
                                                     //拷贝范例配置文件
```

目前phpMyAdmin版本为3.5.2.2。

## 修改config.inc.php配置文件

编辑config.inc.php，将cookie改成http。

```
[root@localhost phpMyAdmin]# vi config.inc.php
/* Authentication type */
$cfg['Servers'][$i]['auth_type'] = 'http';
```

## 启动Apache服务

配置完phpMyAdmin后，需要开启Apache服务，这样就能正常使用phpMyAdmin了。

```
[root@localhost phpMyAdmin]# service httpd start           //启动 Apache
Starting httpd:                                            [  OK  ]
```

## 配置防火墙

phpMyAdmin要使用Apache服务，所以必须在防火墙配置中开启80端口，这样才可以对外连接，除非使用本机的浏览器访问，否则其他计算机就无法访问。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
```

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动防火墙服务，配置才会生效。

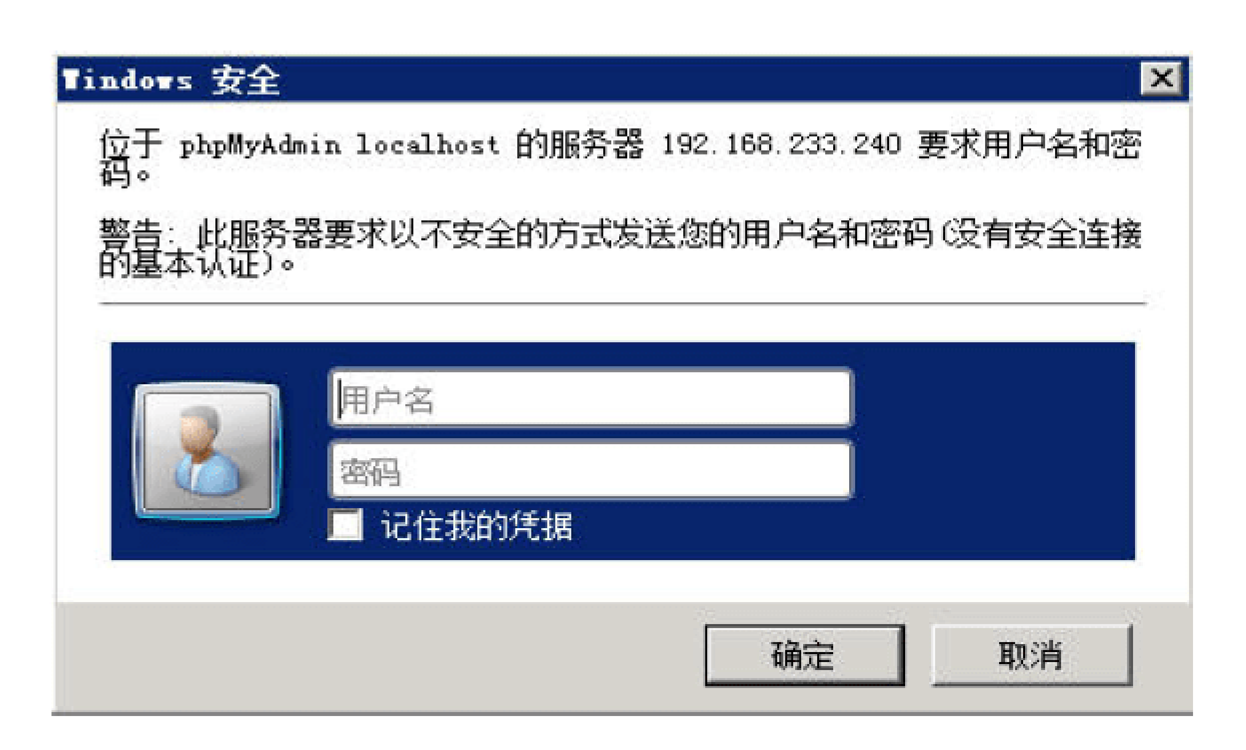
```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                       [  OK  ]
iptables: Setting chains to policy ACCEPT: filter        [  OK  ]
iptables: Unloading modules:                             [  OK  ]
iptables: Applying firewall rules:                       [  OK  ]
```

## 使用phpMyAdmin工具

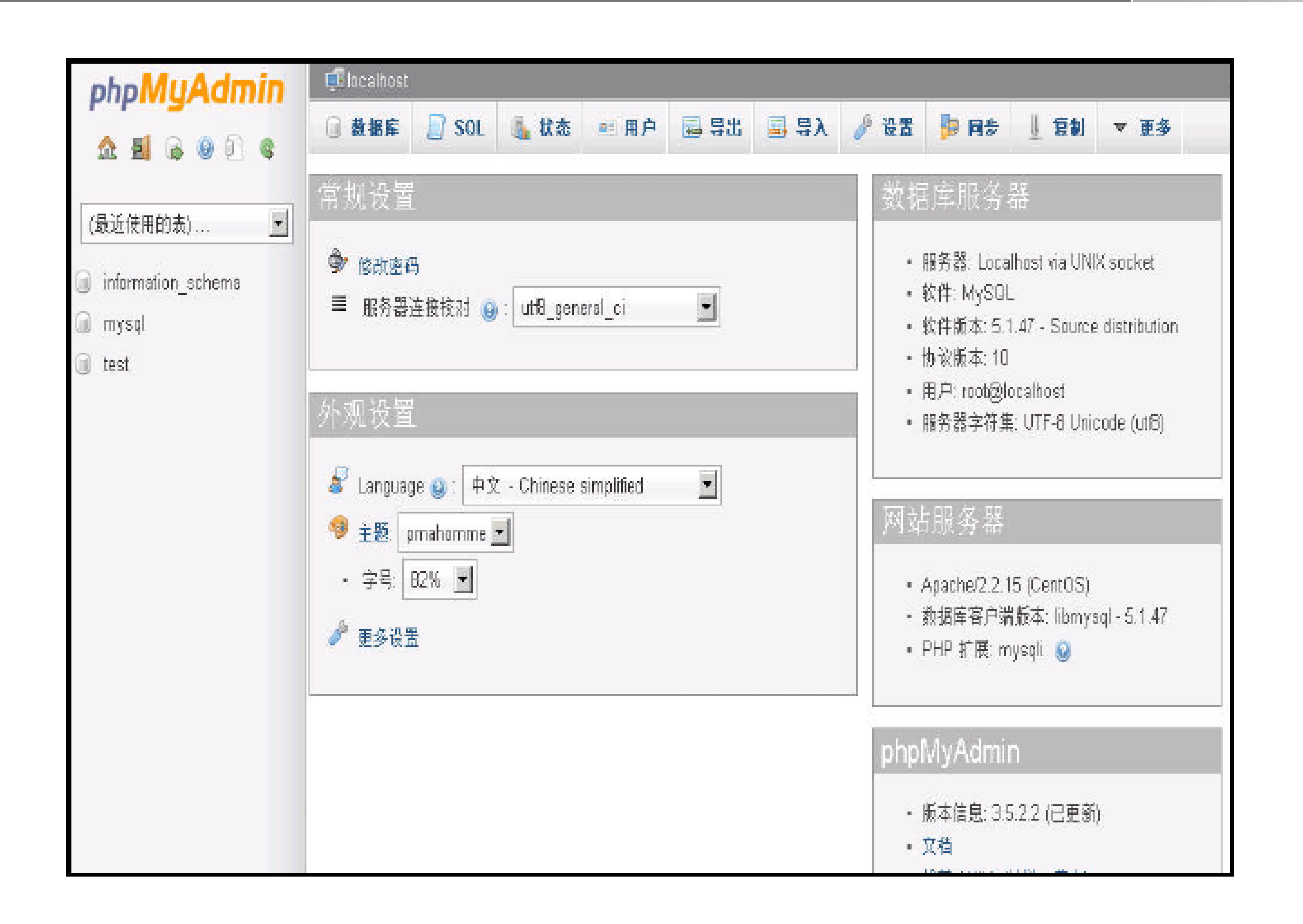
使用前先检查MySQL数据库是否启动，然后检查MySQL数据库是否已配置用户密码，phpMyAdmin必须要有密码才可以使用。

```
[root@localhost ~]# service mysqld status       //查看 MySQL 启动状态
mysqld (pid  1550) is running...
```

一切检查完毕后，在浏览器中输入【http://IP或网址/phpMyAdmin】，默认以root账号登录，若有其他账号需先配置才可以登录。




输入账号和密码后，进入phpMyAdmin主界面。



# 7.5 Navicat for MySQL图形管理工具

虽然可以使用命令方法管理MySQL数据库，但是许多管理命令不是每个管理员都可以记得住的，管理员也不希望这么麻烦地去管理数据库，所以就要靠工具进行有效管理。MySQL数据库管理工具也很多，除了官方提供的管理工具以外，许多人还使用历史悠久的phpMyAdmin工具，但是phpMyAdmin工具不是很好上手，那也没关系，还有一套叫做Navicat for MySQL的管理工具。

Navicat官方网站：http://navicat.com/cn。

Navicat for MySQL为远程操作MySQL数据库的图形化工具，管理员在使用MySQL数据库时多半都因为众多的命令而退缩，phpMyAdmin工具也不是很方便使用，如果习惯Microsoft SQL Server操作的话，那就使用Navicat For MySQL，其使用方法和操作与Microsoft SQL Server相似，这样就比较容易上手。

软件下载网址：http://navicat.com/cn/download/download.html。

该软件有商业版与免费版，但是都可以使用，商业版有完整的功能，不过有30天限制，免费版有部分功能限制，两者功能差异在于备份、报表、日程，若是只是单纯操作MySQL数据库，免费版的功能已经足够了。

## 配置远程管理账号

要远程管理MySQL数据库必须要配置远程管理账号权限，否则就算有账号也无法远程登录，先登录MySQL数据库主机，授权root用户允许IP地址192.168.233.1可以登录MySQL并授予所有权限。

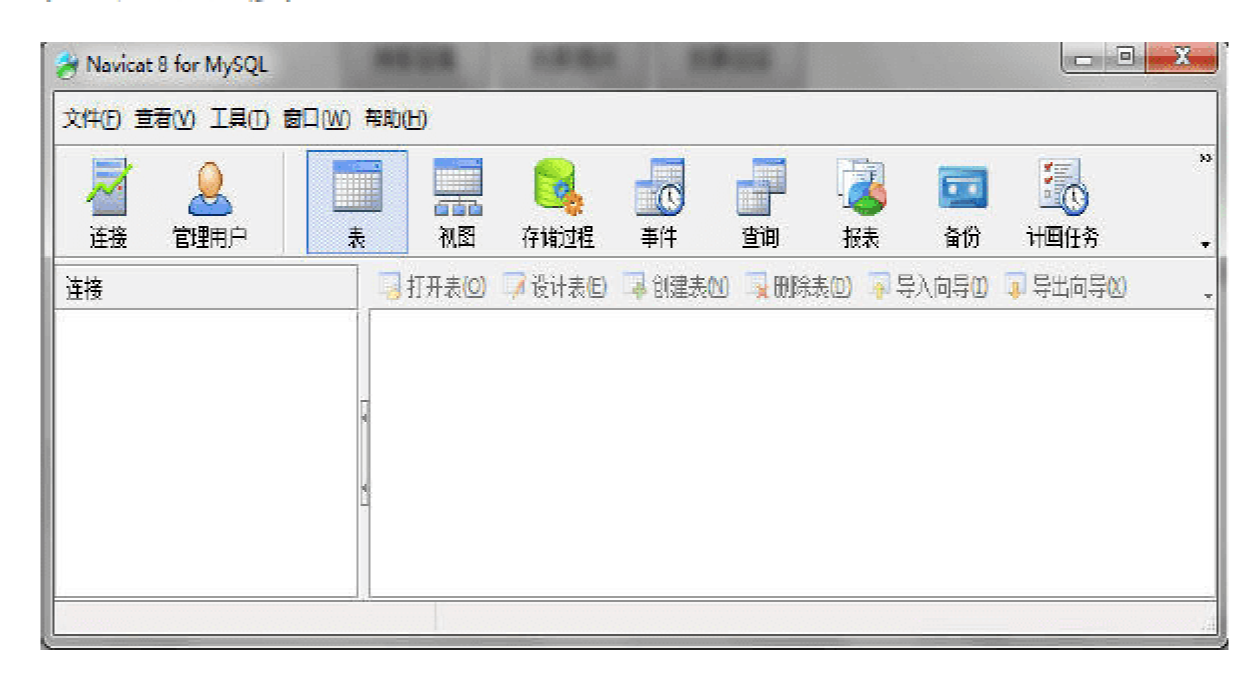
```
[root@localhost ~]# mysql -u root -p      //登录 MySQL
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
```

```
Server version: 5.1.52 Source distribution
Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license

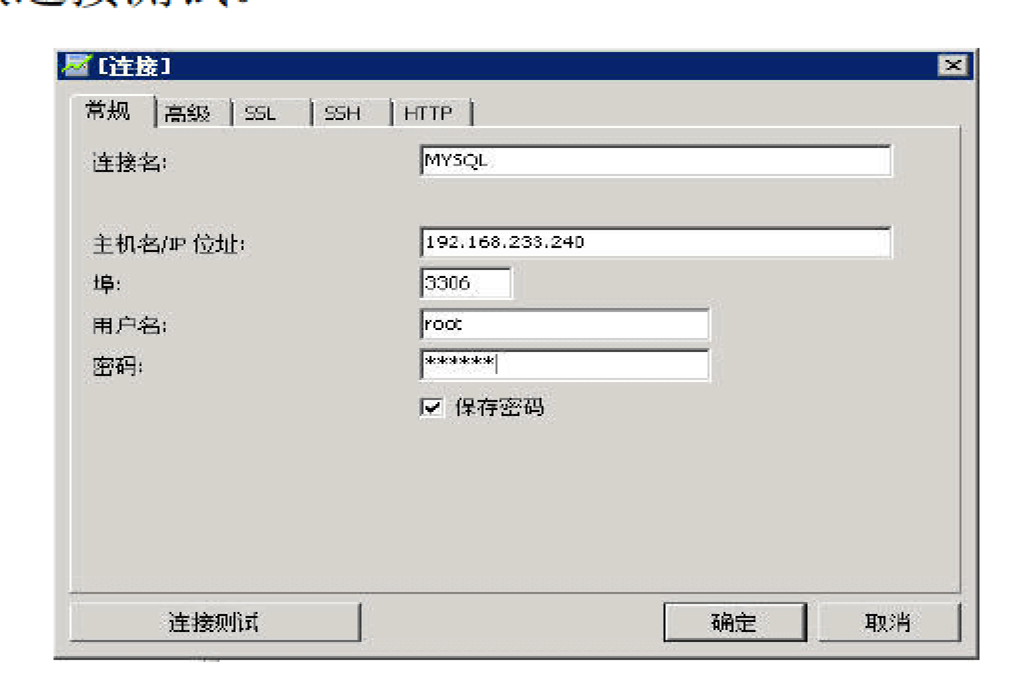
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> grant all privileges on *.* to root@192.168.233.1 identified by 'Aa1234567';
Query OK, 0 rows affected (0.00 sec)     //配置远程管理 IP 地址
mysql> SHOW GRANTS FOR root@192.168.233.1;     //查看用户权限
+-------------------------------------------------------------------------+
| Grants for root@192.168.233.1                                           |
+-------------------------------------------------------------------------+
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'192.168.233.1' IDENTIFIED BY PASSWORD
'*5AF7F0C8FBF 1E7D12F5BFBB4A39032C91A10106'                               |
+-------------------------------------------------------------------------+
1 row in set (0.00 sec)
mysql> quit                  //退出 MySQL
```

## Navicat for MySQL连接配置

这里是使用完整版的Navicat for MySQL，如下图所示，第一次开启没有任何连接的数据库，要连接数据库，单击【连接】。



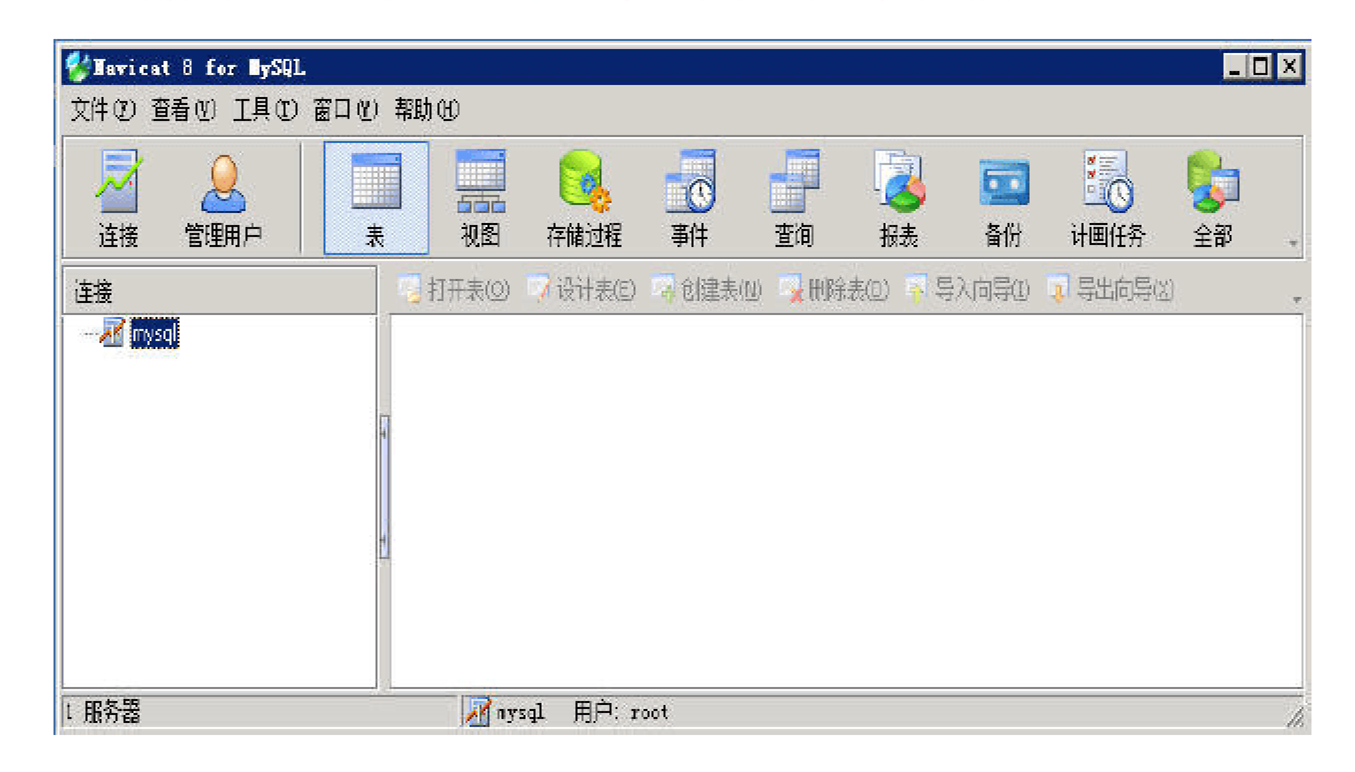

创建一个新的连接窗口，输入连接名称、主机名或MySQL数据库主机的IP地址，端口默认为3306，远程连接用户的用户名为root，输入连接用户密码，输入完毕后，在单击【确定】前，先按【连接测试】做连接测试。



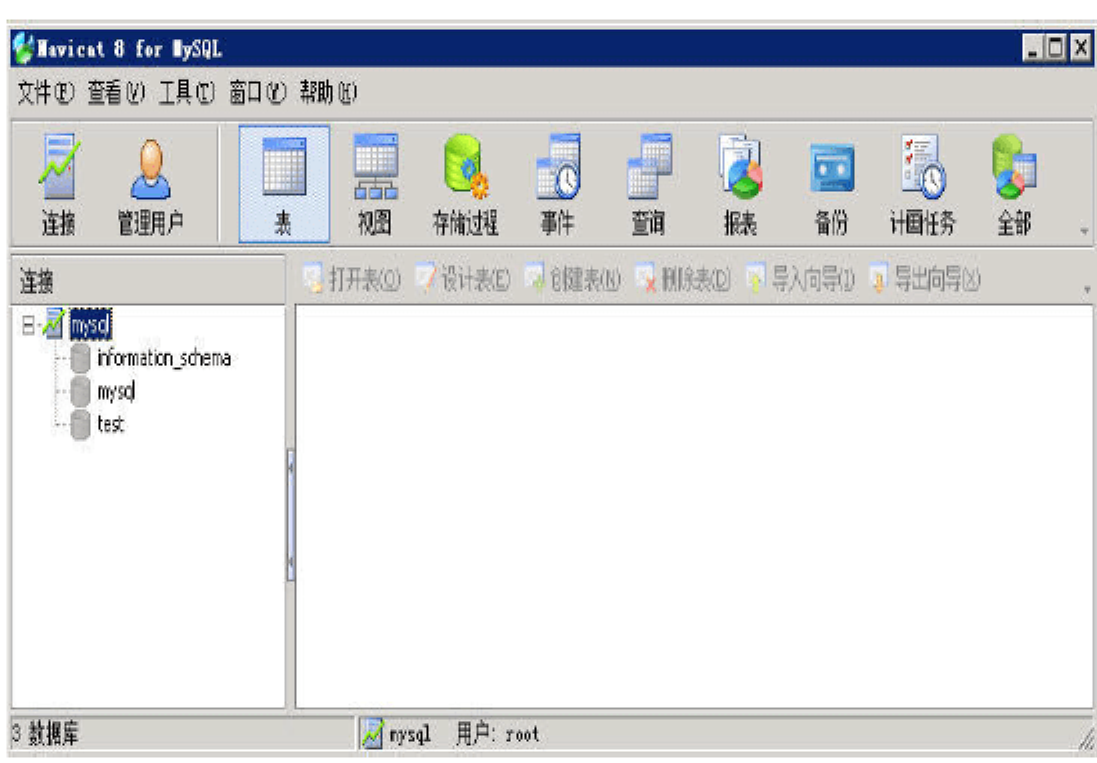
出现下图所示的提示，表示MySQL数据库连接成功，就可以确保配置正确无误。



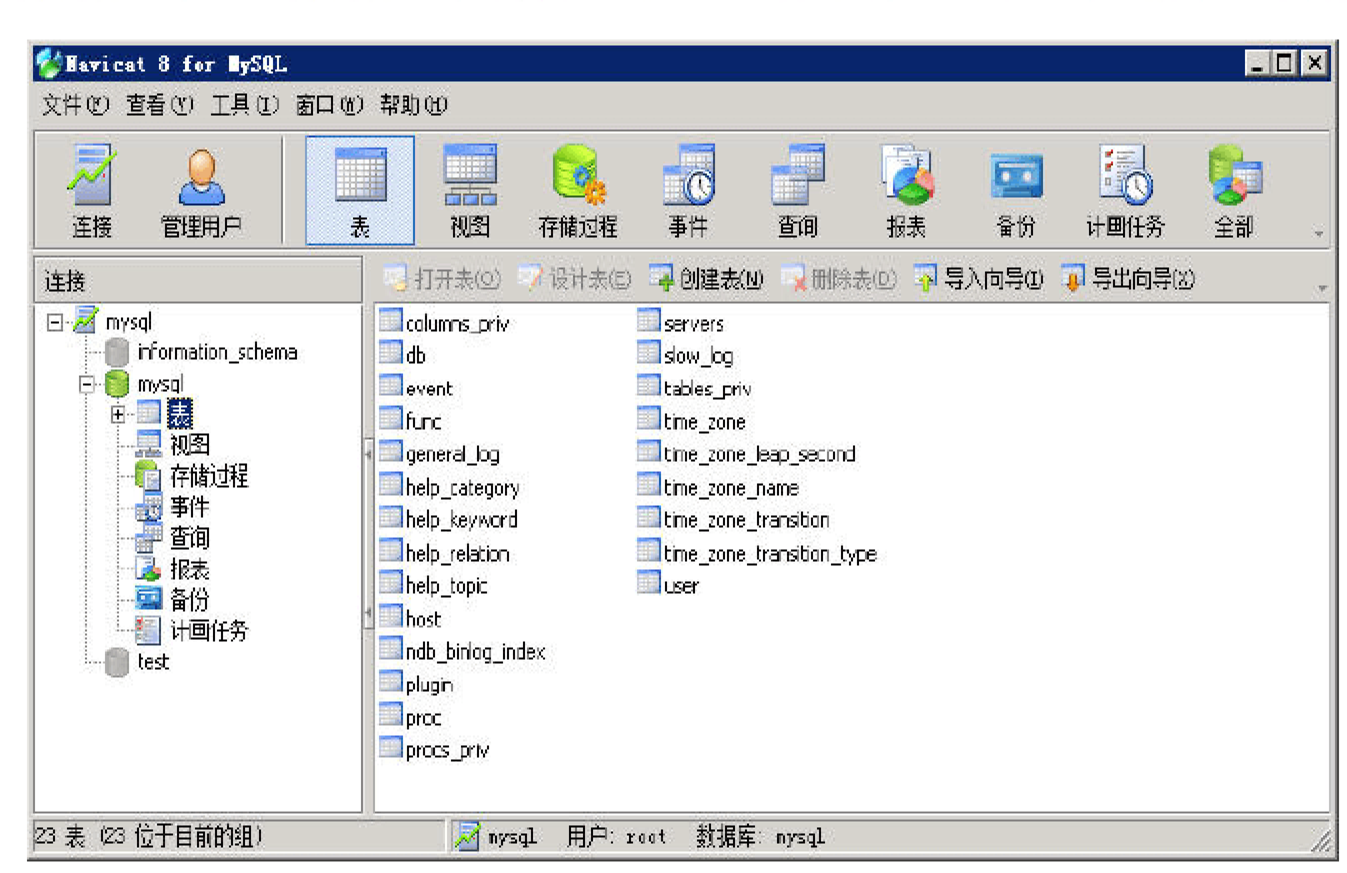

连接成功后，按【确定】，出现连接后的画面，如下图所示。



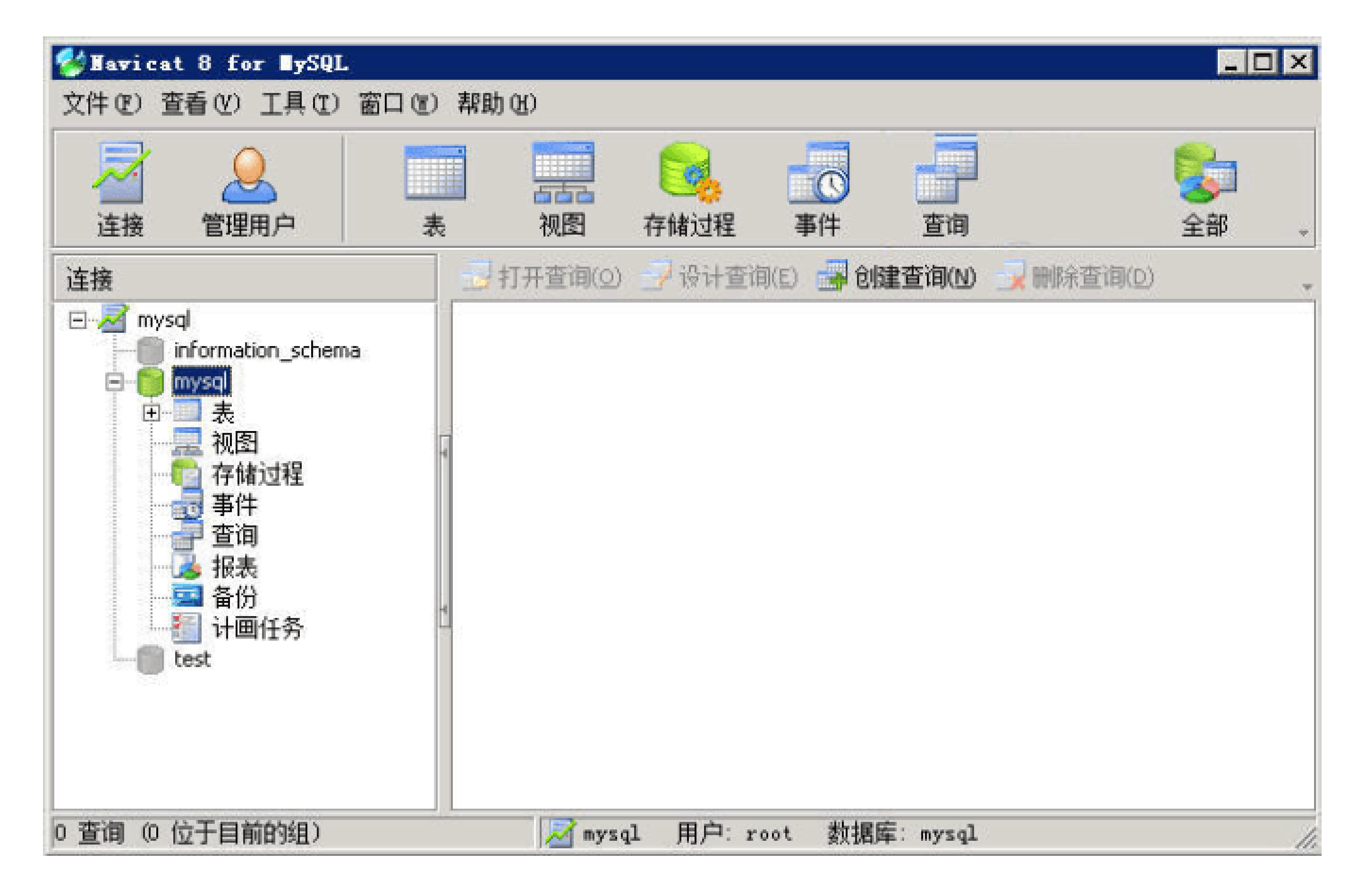

展开连接项目后，就可以看到MySQL数据库内的所有数据库，数据库图标呈灰色表示未点击开启。




展开其中一个数据库后，数据库图标呈绿色，展开后可以看到所有功能选项。



免费版本有功能限制，如报表、备份、计划任务等功能。



# 第8章

# FTP——文件服务器

FTP（File Transfer Protocol）即文件传输协议，可以在不同的计算机之间传输不同类型的文件，如果要在两台不同的计算机之间传输文件，两者必须要使用相同的FTP协议才行。FTP协议是用来规范不同计算机传输文件的共同协议，任何计算机只要遵循此协议，就可以和其他不同的计算机相互传输文件。通过FTP服务就可以在任何两台计算机（不论是否为相同的操作系统）之间互相传输文件。

## 8.1 安装vsftpd

vsftpd全名为Very Secure FTP Daemon，是一款安全性比较高的FTP软件，一般的Linux操作系统都会使用此软件，以下介绍如何安装vsftpd及其基本的配置。

### 检查vsftpd软件

检查是否已经安装vsftpd软件，如果没有任何信息，需自行安装。

```
[root@localhost /]# rpm -qa | grep vsftpd
vsftpd-2.2.2-6.el6_0.1.x86_64
```

### vsftpd安装

安装vsftpd软件，最简单的方法是以yum在线更新进行安装，如果使用源代码编译安装需要到官网下载安装文件。

```
[root@localhost /]# yum install vsftpd -y   //安装vsftpd
Dependencies Resolved
======================================================================
 Package        Arch          Version              Repository       Size
======================================================================
```

```
Installing:
 vsftpd          x86_64       2.2.2-6.el6_0.1        updates         150 k
Transaction Summary
==========================================================================
Install       1 Package(s)
Upgrade       0 Package(s)
Total download size: 150 k
```

## 配置防火墙

Vsftpd软件安装完成后，默认端口是21，所以需在防火墙配置中开启21端口，这样才可以对外连接。

```
[root@localhost /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
                                                              //FTP 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost /]# service iptables restart
iptables: Flushing firewall rules:                        [  OK  ]
iptables: Setting chains to policy ACCEPT: filter         [  OK  ]
iptables: Unloading modules:                              [  OK  ]
iptables: Applying firewall rules:                        [  OK  ]
```

## 启动前的配置

以下两个操作需在启动前进行配置，如果没有配置则无法正常登录vsftpd服务器，如果使用CentOS 6.x之前的版本则只需要关闭SELinux。

第一个命令是解除SELinux保护，否则无法读取FTP目录，输入命令后，显示提示信息Could not change active booleans: Invalid Boolean，表示解除成功，如果不提示此信息代表解除失败，再查看命令是否输入错误，解除成功后，继续输入第二个命令，这个命令会执行一分钟左右，

成功后也不会有任何提示信息。

```
[root@localhost ~]# setsebool ftpd_disable_trans 1
Could not change active booleans: Invalid Boolean
[root@localhost ~]# setsebool -P ftp_home_dir=1
```

如果没有执行第二个操作，当连接到FTP服务器时，会出现无法列出服务器目录的情况。

```
500 OOPS: cannot change directory:/home/jerry
500 OOPS: 500 OOPS: child died
远程主机已关闭连接。
```

为了减少vsftpd服务使用中一些不必要的麻烦，建议将SELinux关闭。

CentOS 6.x之前的vsftpd版本，连接方式默认为被动模式（Passive Mode），CentOS 6.x之后的vsftpd版本，必须经过配置，否则以主动模式（Active Mode）连接，在vsftpd.conf配置文件中添加参数pasv_enable=no，此操作不一定需要，按自己的需求配置即可，建议配置为被动模式（Passive Mode），因为大部分的FTP连接软件默认都是以被动模式连接的，如FileZilla等软件。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
pasv_enable=no                                              //将服务配置为被动模式
```

说明

CentOS 6.0默认为vsftpd-2.2.2，CentOS 5.5为vsftpd-2.0.5。

## 启动vsftpd 服务

确定vsftpd软件已正确安装，接下来就是启动服务，启动完成后，检查vsftpd软件是否监听21端口，为了使用方便，建议将vsftpd服务设为默认启动。

```
[root@localhost /]# service vsftpd start      //启动 vsftpd 服务
Starting vsftpd for vsftpd:                      [  OK  ]
[root@localhost /]# chkconfig vsftpd on       //将 vsftpd 配置为默认启动
[root@localhost /]# netstat -tunlp | grep vsftpd    //检查 vsftpd 运行状态
tcp      0    0 0.0.0.0:21             0.0.0.0:*              LISTEN     4120/vsftpd
```

下表为vsftpd的基本操作。

| 服务状态 | 命令 |
|---|---|
| 启动 vsftpd 服务 | service vsftpd start |
| 关闭 vsftpd 服务 | service vsftpd stop |
| 重新启动 vsftpd 服务 | service vsftpd restart（将服务停止后，再重新启动服务） |
| 重新读取vsftpd配置文件 | service vsftpd reload（重新读取服务器的配置文件） |

# 8.2 修改默认端口

FTP服务的默认端口为21，为了服务器的安全性，通常都会在安装好后进行修改，那为什么Apache安装好后较少修改80端口呢？原因是用户在浏览器中输入网址时，不会加上端口号码，但是FTP服务除了可以以匿名方式连接，也可以使用用户验证方式连接，前提是需告诉用户连接的IP地址、账号、密码和修改后的连接端口，所以才说Web较少修改，FTP服务常常修改，不过建议进行Web修改，降低服务器风险。

## 配置端口

vsftpd默认端口就是21，配置文件内没有修改端口的参数，需在最后一行添加listen_port=port，port是端口号，这里输入端口为2112，输入完成后保存退出。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf     //修改 vsftpd 配置文件
listen_port=2112                  //修改后的端口
```

## 配置防火墙

Vsftpd服务默认端口为21，如果要修改端口，则也需要修改防火墙配置，以便开启修改后的端口，这样才能对外连接。

```
[root@localhost /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp -dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 2112 -j ACCEPT
                                                         //修改后的端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                      [  OK  ]
iptables: Setting chains to policy ACCEPT: filter       [  OK  ]
iptables: Unloading modules:                            [  OK  ]
iptables: Applying firewall rules:                      [  OK  ]
```

## 重新启动vsftpd

Vsftpd配置完成后保存退出，必须重新启动vsftpd服务，配置才会生效。

```
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                          [  OK  ]
Starting vsftpd for vsftpd:                                    [  OK  ]
```

## 测试vsftpd端口

使用FileZilla 软件连接FTP服务时，输入界面将端口改成2112，然后连接FTP服务，会显示连接成功信息，如下图所示。

状态：正在连接 192.168.233.240:2112...
状态：连接建立，等待欢迎消息...

如果FileZilla连接时未将端口修改为2112，则会出现无法连接到服务器的错误信息，如下图所示。

状态：正在连接 192.168.233.240:21...
状态：尝试连接"ECONNREFUSED - Connection refused by server"失败。
错误：无法连接到服务器
状态：正在等待重试...

# 8.3 限制上传下载带宽

FTP服务器的使用效率与服务器带宽有一定的关系，除非你的带宽没有限速，不然还是要限制一下每位用户上传下载的带宽，配置文件中的anon_max_rate参数用于限制匿名用户传输率，local_max_rate参数用于限制本机用户传输率，这里为本机用户，编辑vsftpd配置文件，默认没有local_max_rate参数，需要在配置文件的最后一行添加，这里限制本地用户上传下载都使用300KB，这样上传下载都会以300KB的速度传输。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
local_max_rate=300000                                  //限制本地用户上传下载为 300K
```

**说明**

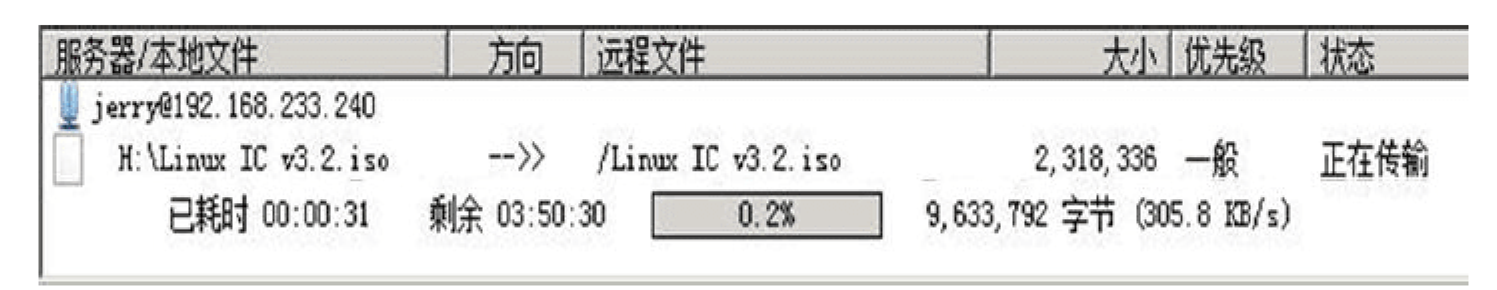
1KB=1000 Btyes。

配置完成后保存退出，重新启动vsftpd服务，这样配置才会生效。

```
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                          [  OK  ]
Starting vsftpd for vsftpd:                                    [  OK  ]
```

## 测试上传下载带宽

使用较大的文件进行测试，如下图所示，速度一般都会维持在300KB左右，这代表配置成功。




# 8.4 配置特定用户的带宽

FTP限制带宽是重要的，不过每个人都配置相同带宽，在内网环境中或许是允许的，但是在实际工作环境中，需要给有些特殊用户配置特殊的带宽，所以配置每个用户使用不同带宽也是管理带宽的方法，编辑vsftpd配置文件，必须创建管理用户带宽的配置文件目录，默认没有此行，需在配置文件中添加，配置完成后保存退出。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
user_config_dir=/etc/vsftpd/limit          //创建管理用户带宽的配置文件目录
```

> **说明**
>
> 管理用户带宽的配置文件路径可以自行配置。

配置文件中指定的用户管理配置文件需要在/etc/vsftpd目录下创建名称为limit的文件夹，默认/etc/vsftpd目录下没有此文件夹，所以必须自行创建，这里要限制ken用户只能以300KB的速度上传下载，必须创建针对ken用户带宽限制的配置文件。

```
[root@localhost ~]# mkdir /etc/vsftpd/limit  //创建管理用户带宽的配置文件文件夹
[root@localhost ~]# vi /etc/vsftpd/limit/ken //创建针对 ken 用户带宽限制的配置文件
local_max_rate=300000             //配置 ken 用户带宽 300KB
```

> **说明**
>
> 配置前先确认服务器有ken用户。

配置完成后保存退出，重新启动vsftpf服务，这样配置才会生效。

```
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
```

## 测试特定用户的带宽

以账号ken登录，测试是否有限制带宽，限制传输带宽大约为300KB。

ken@192.168.233.240
H:\CentOS-6.0-x86_64-...　-->>　/home/ken/CentOS-6.0-x86_...　4,238,80...　一般　正在传输
已耗时 00:00:31　剩余 03:50:30　0.2%　9,633,792 字节 (305.8 KB/s)

以账号jerry登录，该用户没有限制带宽，传输带宽到达29.3MB，代表配置成功。

jerry@192.168.233.240
H:\CentOS-6.0-x86_64-...　-->>　/CentOS-6.0-x86_64-bin-DV...　4,238,80...　一般　正在传输
已耗时 00:00:18　剩余 00:02:06　13.9%　592,642,048 字节 (29.3 MB/s)

# 8.5 限制客户端可连接的IP地址

FTP主机可以限制客户端可连接的网段或IP，利用tcp_wrappers、host.deny及host.allow参数来限制，这里配置为限制所有网段都不可以连接，只有192.168.233的网段才可以连接，先确定配置文件中tcp_wrappers 参数的配置是否为YES，vsftpd默认就为YES，如果为NO，则会对host.deny及host.allow文件有影响。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
tcp_wrappers=YES                 //检查是否为 YES
```

首先配置host.deny文件，限制所有网段都不能连接，配置完成后，保存退出。

```
[root@localhost /]# vi /etc/hosts.deny     //编辑限制配置文件
#
# hosts.deny    This file contains access rules which are used to
#               deny connections to network services that either use
#               the tcp_wrappers library or that have been
#               started through a tcp_wrappers-enabled xinetd.
#
#               The rules in this file can also be set up in
#               /etc/hosts.allow with a 'deny' option instead.
#
#               See 'man 5 hosts_options' and 'man 5 hosts_access'
#               for information on rule syntax.
#               See 'man tcpd' for information on tcp_wrappers
#
vsftpd:all:Deny                  //限制所有网段都不可以连接
```

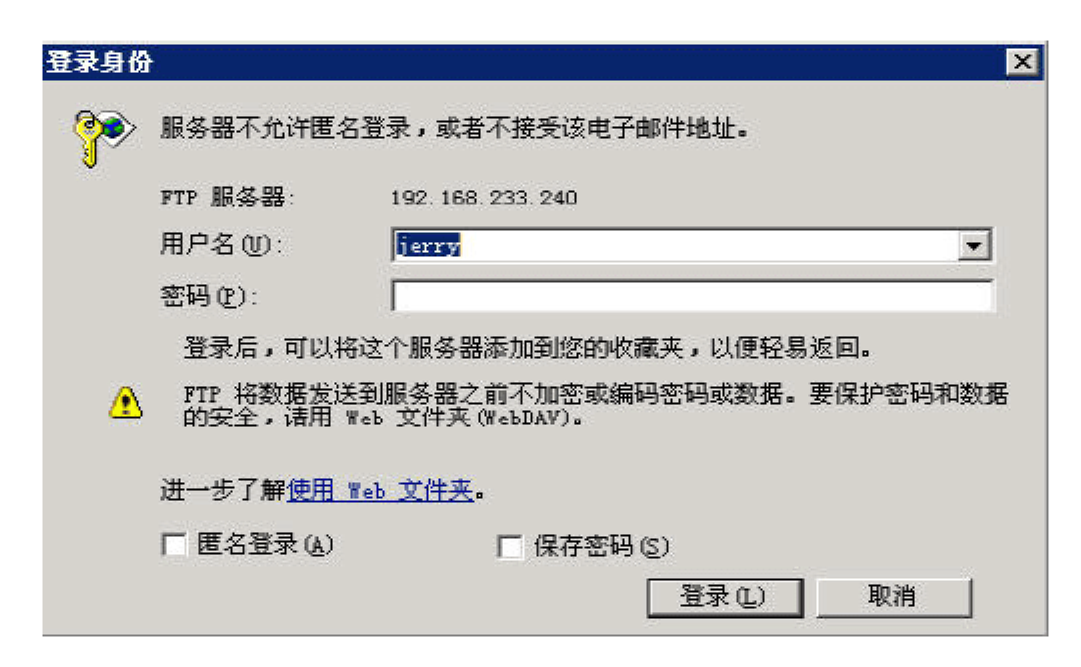
接下来编辑host.allow文件，允许192.168.223网段可以连接，配置完成后，保存退出，由于不是修改vsftpd配置文件，所以无需重新启动vsftpd服务。

```
[root@localhost /]# vi /etc/hosts.allow    //编辑允许连接的配置文件
#
# hosts.allow   This file contains access rules which are used to
#               allow or deny connections to network services that
#               either use the tcp_wrappers library or that have been
#               started through a tcp_wrappers-enabled xinetd.
```

```
#
#               See 'man 5 hosts_options' and 'man 5 hosts_access'
#               for information on rule syntax.
#               See 'man tcpd' for information on tcp_wrappers
#
vsftpd:192.168.233.*:Allow        //开放 192.168.233 网段可以连接
```

## 测试限制IP地址是否成功

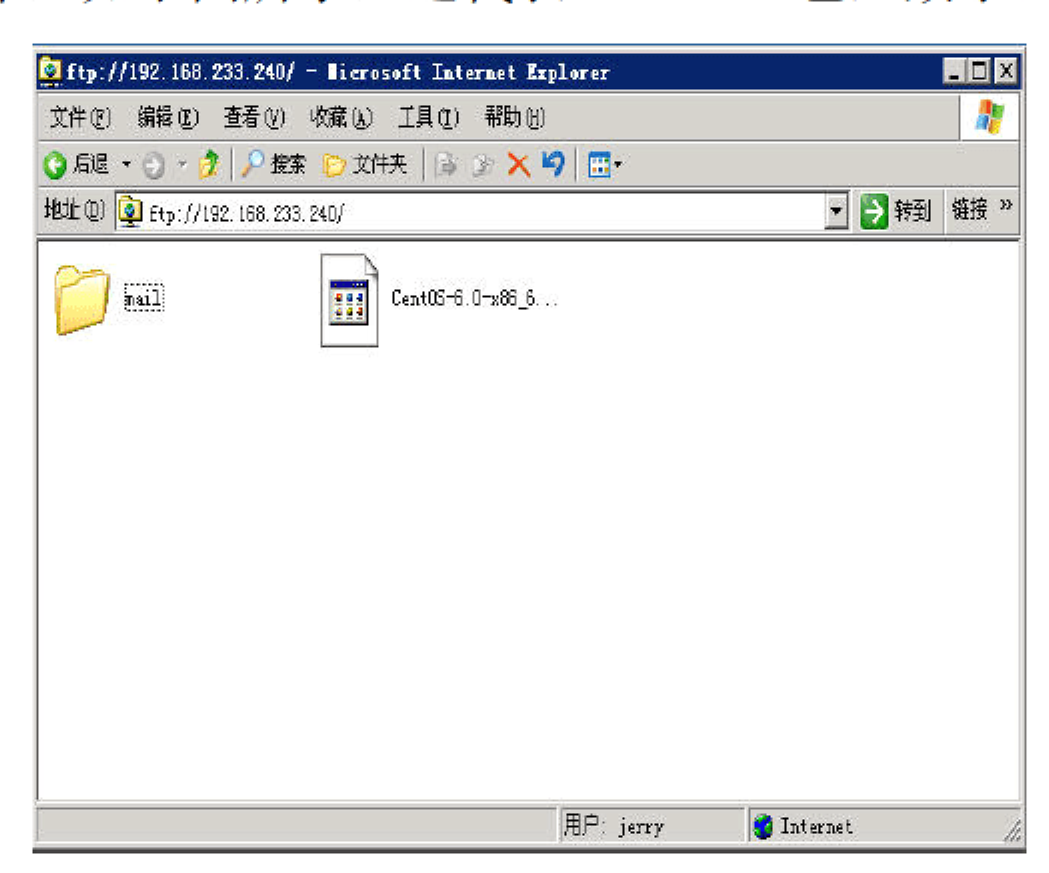
配置完成后，测试限制是否成功，先测试192.168.233网段以外的IP地址，打开浏览器输入vsftpd服务器的IP地址，出现输入用户名和密码界面，如下图所示，无论输入几次都无法进入，就代表host.deny生效。




用命令提示符连接FTP服务器会出现连接中断信息。

```
C:\Documents and Settings\Administrator>ftp 192.168.233.240
Connected to 192.168. 233.240.
421 Service not available.
Connection closed by remote host.
```

接下来测试192.168.233的网段，在浏览器中输入vsftpd服务器IP地址，输入用户名和密码后，即可以正常登录操作，如下图所示，这代表host.allow也生效了。




用命令提示符连接，输入用户名和密码后可以正常登录。

```
C:\>ftp 192.168.233.240
Connected to 192.168.233.240.
220 (vsftpd 2.2.2)
User (192.168.233.240: (none) ) : anonymous
331 Please specify the password.
Password:
230 Login successful.
ftp>
```

```
状态:  正在连接 192.168.233.240:21...
状态:  连接建立，等待欢迎消息...
响应:  220 Welcome to blah FTP service.
命令:  USER jerry
响应:  530 Permission denied.
错误:  无法连接到服务器
状态:  正在等待重试...
```

```
状态:  正在连接 192.168.233.240:21...
状态:  连接建立，等待欢迎消息...
响应:  220 Welcome to blah FTP service.
命令:  USER ken
响应:  331 Please specify the password.
命令:  PASS ***
响应:  230 Login successful.
命令:  OPTS UTF8 ON
响应:  200 Always in UTF8 mode.
状态:  已连接
状态:  读取目录列表...
命令:  PWD
响应:  257 "/home/ken"
```

# 8.6 限制黑名单用户

Vsftpd有配置黑名单功能，可以限制服务器内哪些用户不能登录，为什么要限制用户不能登录呢？原因是主机内有很多用户，不一定每个用户都可以登录FTP主机，不过删除账号又可能影响其他服务的运行，所以就将其加入黑名单，在登录FTP时就会依照黑名单信息拒绝登录。系统默认已经将一些与FTP无关的账号加入在内，配置文件内的userlist_enable参数，默认为YES，是为了限制系统黑名单用户登录，如果设为NO就不会去检查黑名单。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
userlist_enable=YES                          //默认为 YES，如果为 NO，则黑名单不生效
```

默认限制的账号，其实都是系统内建的账号，都没有必要登录FTP，最重要的是root也限制在内，这样主机比较安全，这里加入了jerry为限定用户。

```
[root@localhost ~]# vi /etc/vsftpd/user_list     //编辑黑名单
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default) , never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
# for users that are denied.
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
inobody
jerry                      //新增的限制帐号
```

## 测试黑名单

使用jerry账号登录，测试是否生效，如果成功会出现530 Permission denied无法登录。

使用tom账号登录，直接就可以登录成功。

因为该用户没有在黑名单中。

## 8.7 允许匿名登录，不允许普通用户登录

通常FTP主机为公用的服务，主机默认配置使用匿名登录，不开放普通用户，主要是为防止普通用户登录后，对其他用户的目录做错误操作。

匿名用户anonymous_enable参数及普通用户local_enable参数默认为YES，都是允许登录，将普通用户local_enable参数设为NO，普通用户就无法登录。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
# Allow anonymous FTP?（Beware - allowed by default if you comment this out）.
anonymous_enable=YES                    //默认为 YES，启用匿名登录，设为 NO 则关闭
#
# Uncomment this to allow local users to log in.
local_enable=NO                         //默认为 YES，启用普通用户登录，设为 NO 则关闭
```

配置完成后，必须要重新启动vsftpd服务，配置才会生效。

```
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                         [  OK  ]
Starting vsftpd for vsftpd:                                   [  OK  ]
```

### 测试是否已禁止普通用户登录

以账号jerry登录，系统则会出现530 This FTP server is anonymous only信息，说明只有匿名（anonymous）账号才可以登录，该用户无法登录FTP服务器。

```
C:\Users\jerry>ftp 192.168.233.240
已连接到 192.168.233.240。
220（vsftpd 2.2.2）
用户（192.168.233.240:（none））: jerry
530 This FTP server is anonymous only.                  //只有匿名可以登录
登录失败。
```

以匿名账号登录，系统则出现230 Login successful，表示匿名登录成功。

```
C:\Users\jerry>ftp 192.168.233.240
已连接到 192.168.233.240。
220（vsftpd 2.2.2）
用户（192.168.233.240:（none））: anonymous
331 Please specify the password.
密码:
230 Login successful.
```

> **说明**
> 匿名用户登录FTP服务器时需要输入默认匿名用户名（anonymous），不用输入密码。

# 8.8 禁止匿名登录

默认匿名用户anonymous可以登录FTP，不过通常为了安全性都会禁止匿名用户登录，为方便管理，anonymous_enable参数默认为YES启动，将之设为NO禁止，匿名用户就无法登录。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=NO          //默认为 YES 允许匿名用户登录，NO 则匿用户名无法登录
#
# Uncomment this to allow local users to log in.
local_enable=YES
```

配置完成后，必须要重新启动vsftpd服务，配置才会生效。

```
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
```

## 测试是否已禁止匿名用户登录

使用匿名用户登录，输入匿名用户名anonymous即出现530 Login incorrent错误信息，该信息表示匿名用户无法登录。

主机(H): 192.168.233.240 用户名(U): anonymous 密码(W): 端口(P):
响应: 220 Welcome to blah FTP service.
命令: USER anonymous
响应: 331 Please specify the password.
命令: PASS **************
响应: 530 Login incorrect.
错误: 严重错误
错误: 无法连接到服务器

# 8.9 限制一个IP连接的数量

限制每个IP的连接数是必要的，如果一个IP地址对主机连接太多，只会让主机耗费不必要的资源，不过在配置时要考虑一下FTP是配置在内部还是在公网上使用，因为很多公网IP对应内网多个内部IP，所以对连接数的设置就要有所考虑，vsftpd配置文件默认没有限制连接数量（数字0代表无限制），或者根本没有此行，自己在最后一行加入max_per_ip=连接数即可，这里设为3，一个IP超过3个连接数就无法登录。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
max_per_ip=3                                               //配置连接数量
```

配置完成后，必须要重新启动vsftpd服务，配置才会生效。

```
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                      [  OK  ]
```

```
Starting vsftpd for vsftpd:                                [  OK  ]
```

## 测试连接数量

使用FileZilla FTP Client进行连接，在第四个连接时，出现421 There are too many connections from your internet address信息，这时必须将其他连接关闭才可以连上FTP。

```
状态:  正在连接 192.168.233.240:21...
状态:  连接建立，等待欢迎消息...
响应:  421 There are too many connections from your internet address.
错误:  无法连接到服务器
状态:  正在等待重试...
状态:  正在连接 192.168.233.240:21...
状态:  连接建立，等待欢迎消息...
响应:  421 There are too many connections from your internet address.
错误:  无法连接到服务器
```

> **说明**
>
> 在vsftpd.conf中配置max_clients=连接数，与配置max_per_ip=连接数结果相同。

# 8.10 限制空闲时间过久即断线

不管何种服务器，很多连接上来的用户都会在空闲状态下一直连接，这样会消耗主机的资源，所以就有必要配置空闲时间过久的连接必须中断，默认秒数为300，idle_session_timeout=300，但是该行没有启用，需要删除#号，这里配置空闲30秒没有任何操作即中断连接，将批注#号删除，并将秒数设成30，然后保存退出。

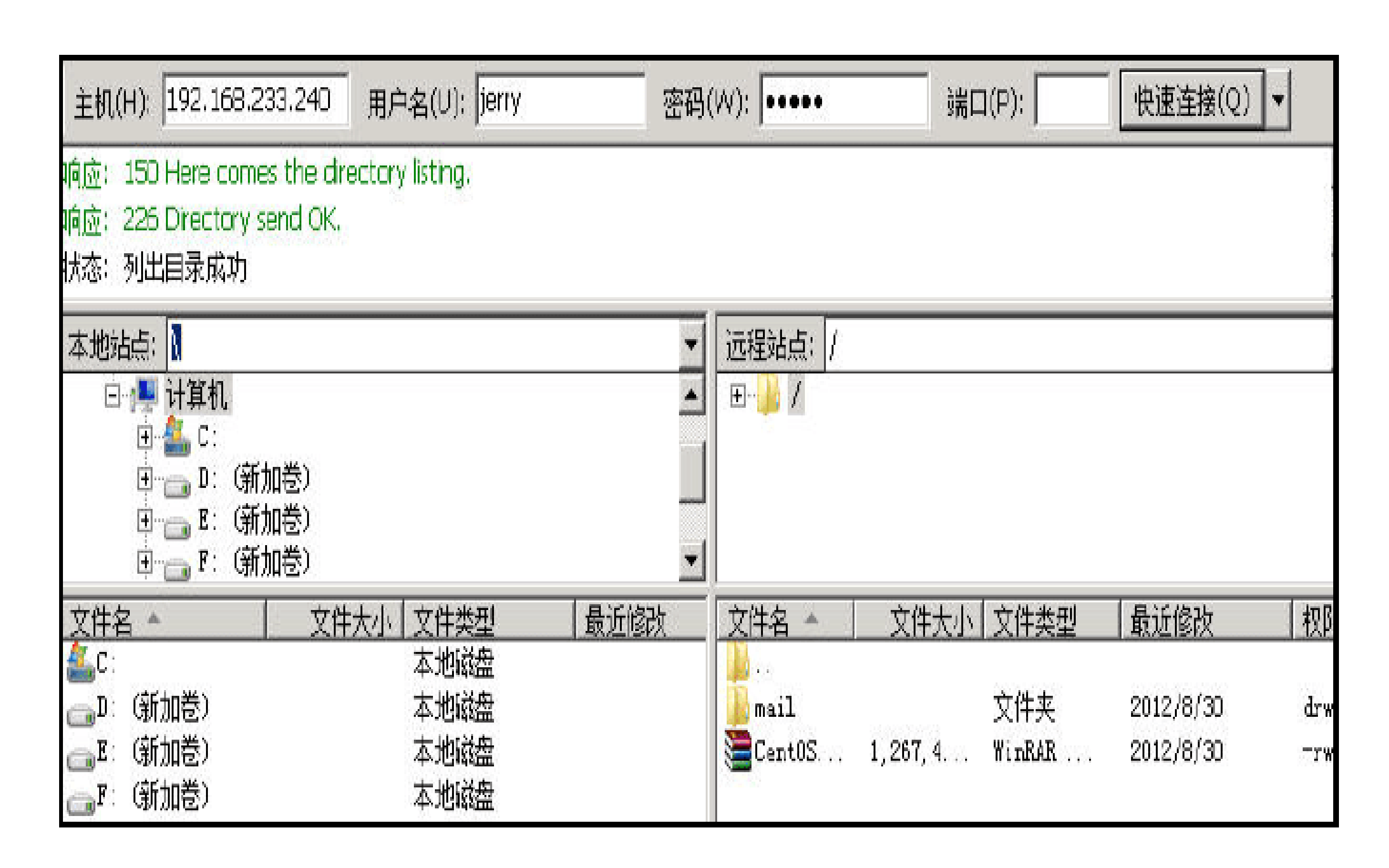
```
 [root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
# You may change the default value for timing out an idle session.
idle_session_timeout=30         //默认不启用，秒数为 300 秒修改为 30，删除#号启动
```

配置完成后，必须要重新启动vsftpd服务，配置才会生效。

```
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
```

## 测试闲置30秒后是否中断连接

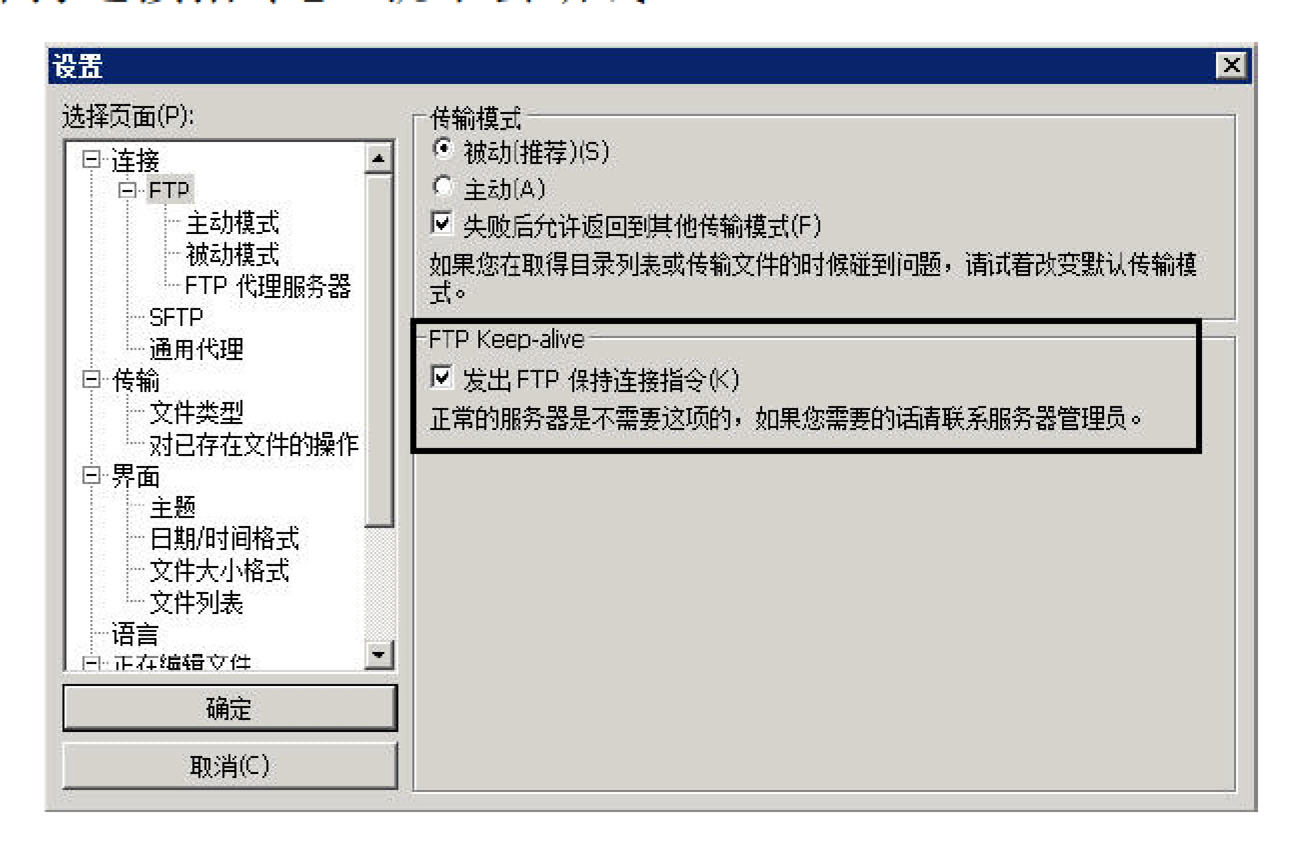
以jerry账号登录后，不做任何动作等待30秒。



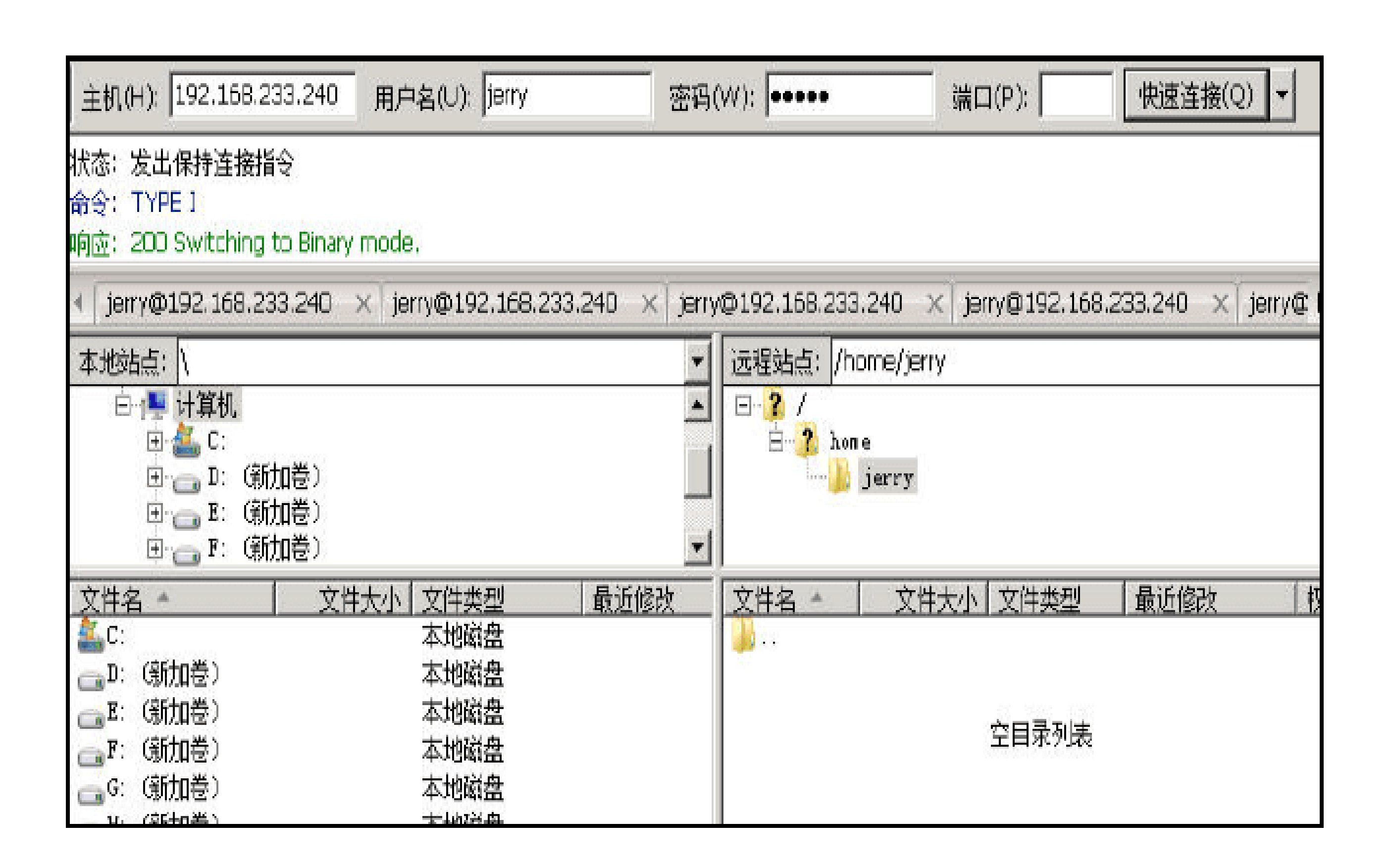

30秒之后，FileZilla FTP Client出现421 Timeout中断连接，信息显示服务器关闭连接。




假如没有关闭连接，原因是目前FTP连接软件会自动帮你重新连接，永不关闭，以FileZilla FTP Client为例，在【设置】的【选择页面】中选择【连接】下面的【FTP】选项，在【FTP Keep-alive】中勾选【发出FTP保持连接指令】，就不会断线。




经过测试发现确实有自动连接现象，FTP软件每隔一段时间就会自动保持连接，为了提高FTP效率，建议关闭空闲连接，如果vsftpd配置了Client连接数的话，太多用户连接在上面，也会导致其他用户无法登录。




# 8.11 禁止用户切换目录

配置FTP服务后，某些情况下，只能允许用户看到自己的目录而不能浏览其他目录，所以就必须做些配置，否则默认情况下，FTP用户拥有读取主机上其他目录的权限，为了服务器的安全还是配置该用户只能浏览自己的目录，CentOS 6.0默认有此配置但未启用，CentOS 6.0以前的版本必须自行输入。

## 限制所有用户不可以切换目录

编辑vsftpd配置文件，先找到chroot_local_user这一行，将#号删除。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
# You may specify an explicit list of local users to chroot () to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot () .
chroot_local_user=YES                          //默认不启用，将#号删除后启用
```

配置完成后，必须要重新启动vsftpd服务，配置才会生效。

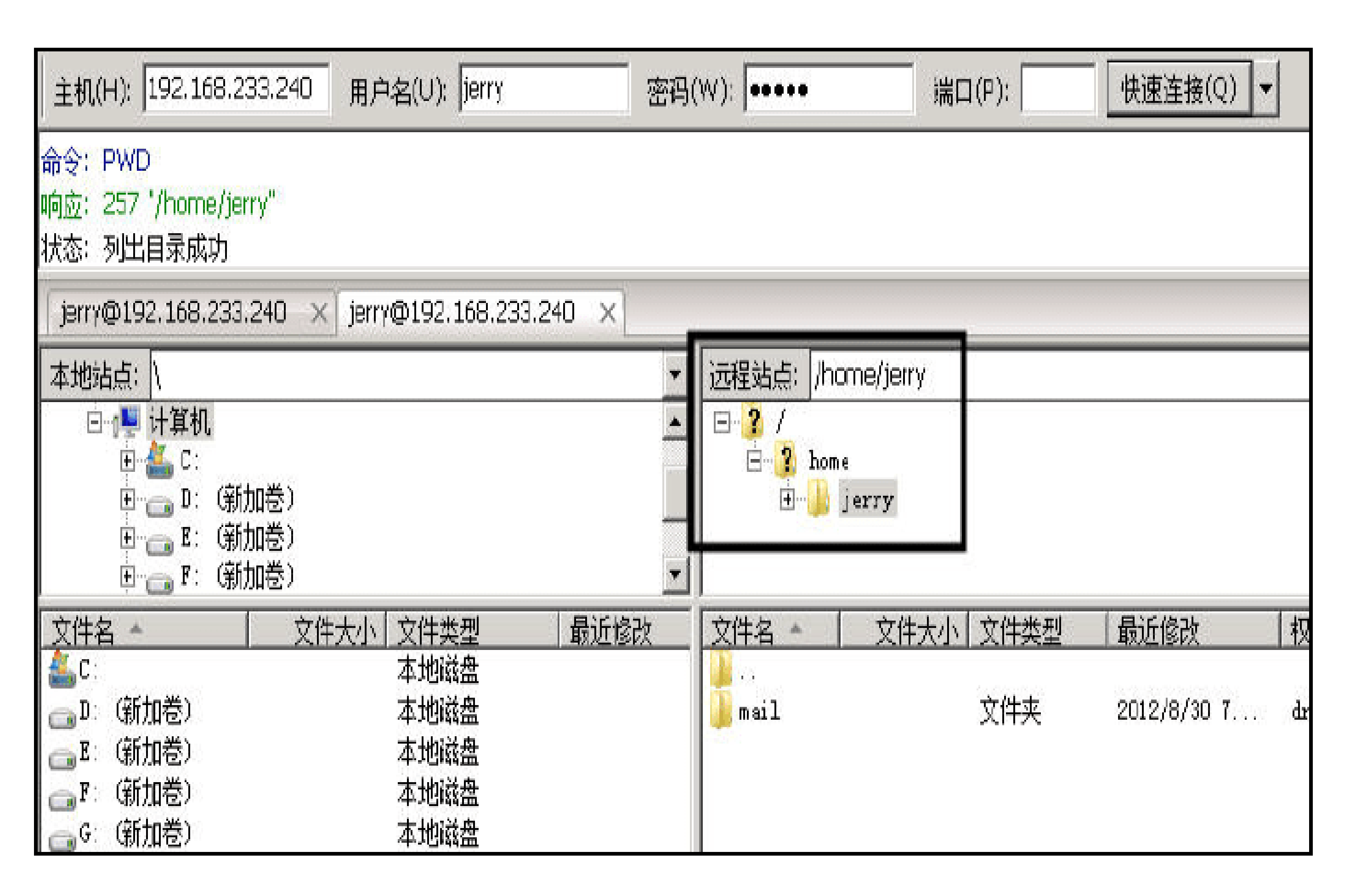
```
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                         [  OK  ]
Starting vsftpd for vsftpd:                                   [  OK  ]
```

## 测试是否已限制所有用户切换目录

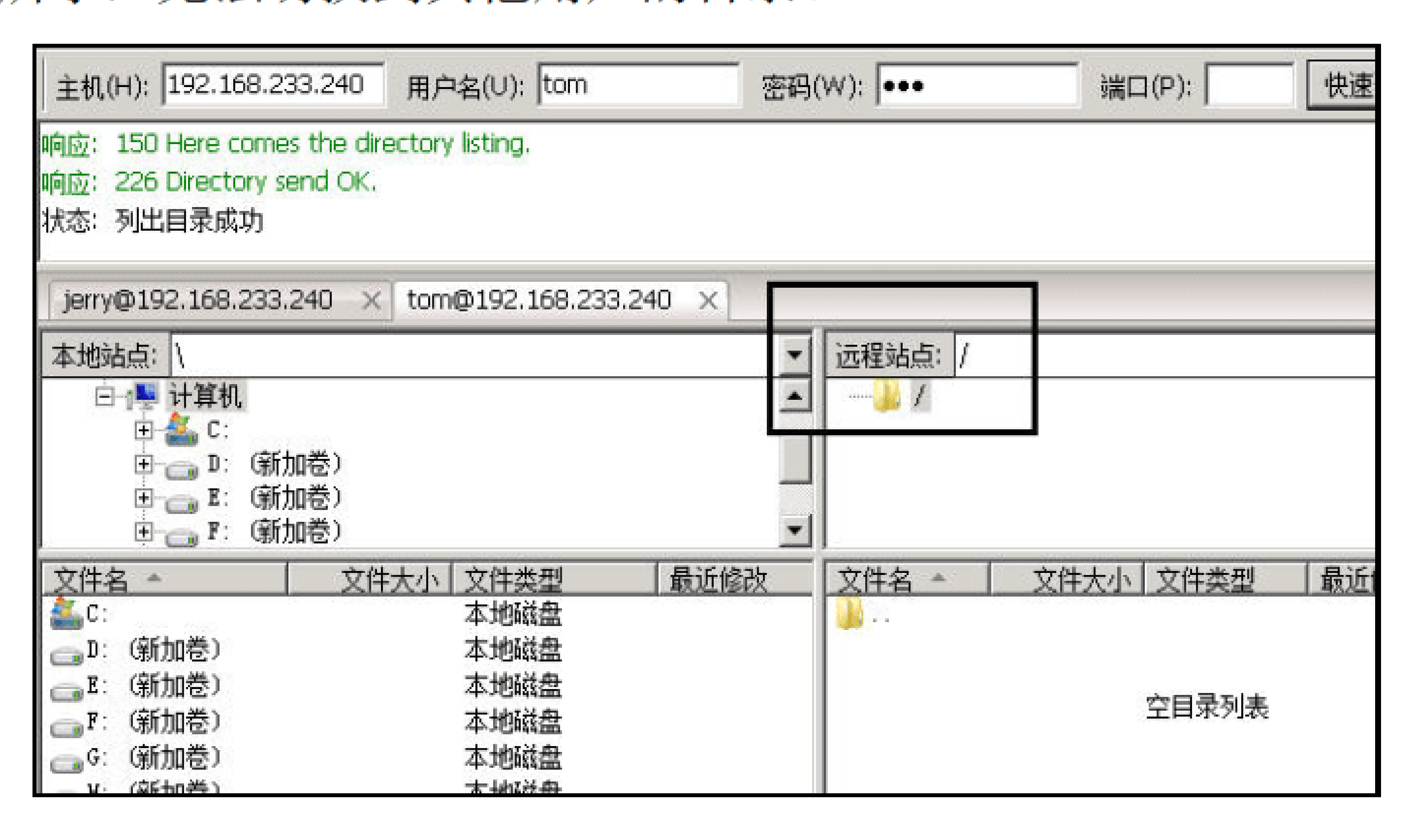
目前home目录下有两个用户jerry和tom。

```
[root@localhost ~]# ll /home
total 8
drwx------. 3 jerry jerry 4096 Aug 20 08:51 jerry
drwx------. 2 tom   tom   4096 Aug 20 11:08 tom
```

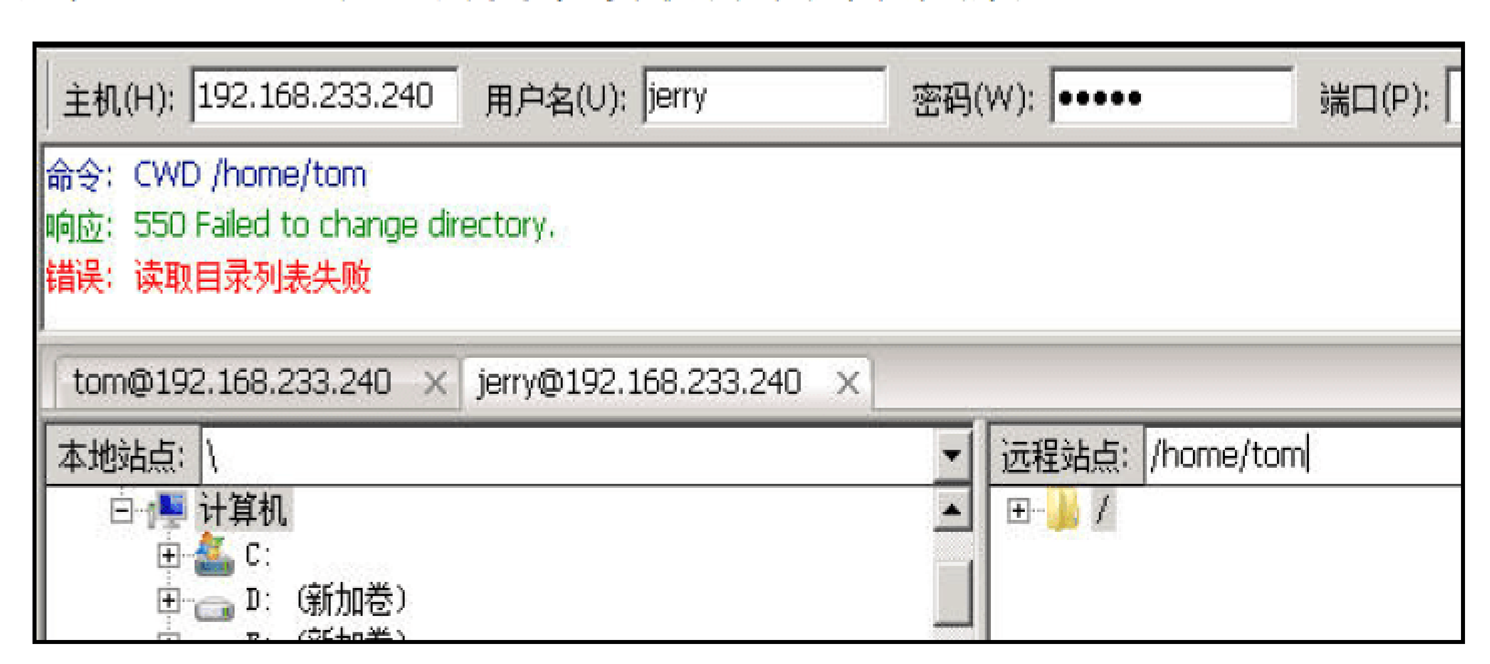
利用FTP连接软件FileZilla FTP Client进行连接，默认vsftpd配置文件中没有加上chroot_local_user=YES，或者将此参数值修改为NO时，可以显示完整的目录路径，以jerry登录就会有/home/jerry完整目录路径。




Vsftpd配置文件中加上chroot_local_user=YES后，不管以哪个用户登录都只能看到该用户的目录，如下图所示，无法切换到其他用户的目录。




如果要强制切换到其他用户目录下，会出现错误信息550 Failed to change directory，若jerry账号要强制切换到/home/tom下，会提示读取目录列表失败。



## 限制特定用户不可以切换用户目录

上述方式是限制所有FTP登录的用户都不能切换到其他用户目录，假设要配置特定用户不可以切换，就要配置禁止名单，建议FTP主机配置所有用户都不能切换目录，若要配置特定用户不能切换就要编辑两个文件vsftpd.conf和chroot_list，先编辑vsftpd.conf，将chroot_list_enable=YES的#号删除，然后保存退出。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
chroot_list_enable=YES                          //默认为不启用，删除#号则启用
```

在/etc/vsftpd下创建一个chroot_list文件，添加要禁止的用户，这里输入jerry作为禁止切换目录的用户名单。

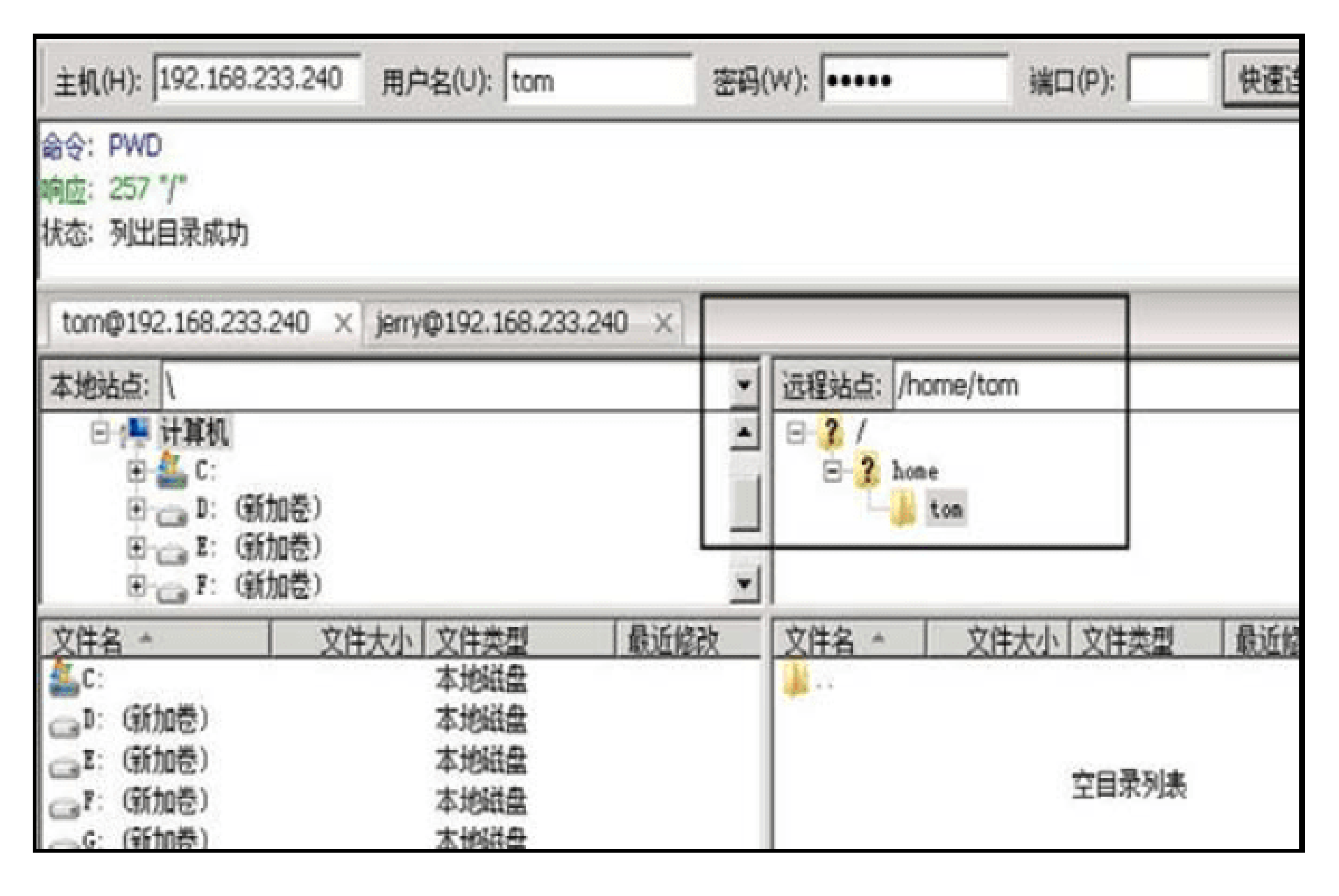
```
[root@localhost ~]# vi /etc/vsftpd/chroot_list
jerry
```

配置完成后，必须重新启动vsftpd服务，配置才会生效。

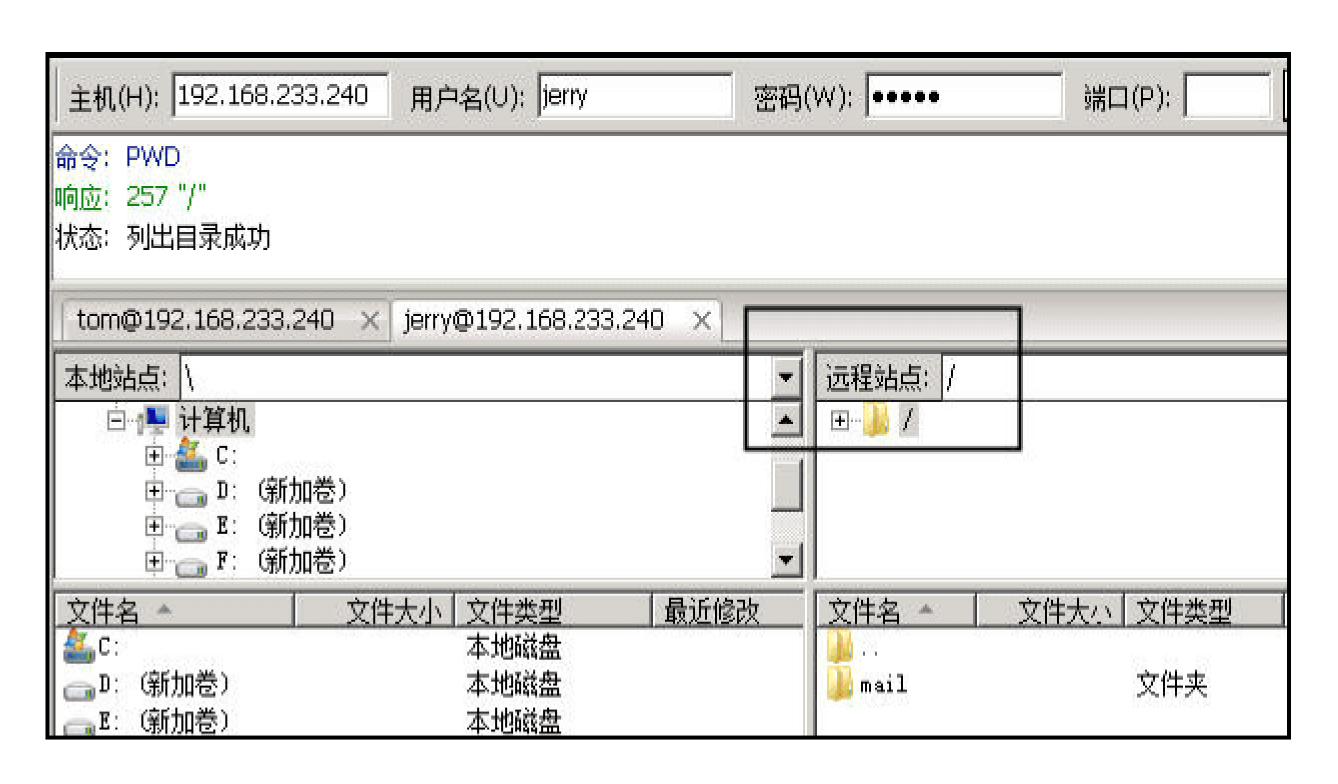
```
[root@localhost ~]# service vsftpd restart
Shutting down vsftpd:                                         [  OK  ]
Starting vsftpd for vsftpd:                                   [  OK  ]
```

## 测试是否已限制单一用户切换目录

以Tom账号登录，可以显示/home/tom完整路径。




以Jerry账号登录后，只能看到Jerry根目录。




FTP配置文件中chroot_local_user参数和chroot_list_enable参数是不可以同时使用的，如果同时使用，本来chroot_list所配置的用户则变成可以显示完整路径，没有配置的用户却会变成无法显示路径，但结果刚好相反。

# 8.12 Vsftpd 使用 SSL/TLS加密传输

为vsftpd服务加上SSL可以提高FTP的安全性，这就类似将Apache的http配置成https，让vsftpd成为加密的FTP服务器。

## 安装OpenSSL

首先检查是否已安装OpenSSL，vsftpd使用SSL/TLS，必须要安装OpenSSL。

```
[root@localhost certs]# rpm -qa |grep openssl //检查是否安装 OpenSSL
openssl-1.0.0-4.el6_0.2.x86_64
```

如果没有安装OpenSSL，对vsftpd配置完SSL后会无法启动，出现force_local_logins_ssl=YES错误。

```
[root@localhost ~]# yum install -y openssl    //安装 OpenSSL
Dependencies Resolved
========================================================================
 Package          Arch        Version              Repository        Size
========================================================================
Updating:
 openssl        x86_64      1.0.0-4.el6_0.2        updates         1.4 M
Transaction Summary
========================================================================
Install       0 Package(s)
Upgrade       1 Package(s)
Total download size: 1.4 M
```

## 创建凭证CA

安装OpenSSL后默认没有任何凭证，可以利用OpenSSL生成一组凭证供暂时使用，产生的

凭证存放路径为/etc/pki/tls/certs，以命令方式生成凭证，输入相关信息后，会生成一个pem文件，然后将这个文件设为只读。

```
[root@localhost ~]# cd /etc/pki/tls/certs      //进入/etc/pki/tls/certs
[root@localhost certs]# openssl req -x509 -nodes -newkey rsa:1024 -keyout
/etc/pki/tls/certs/vsftpd.pem -out /etc/pki/tls/certs/vsftpd.pem
                                              //创建 Vsftpd 凭证
Generating a 1024 bit RSA private key
.++++++
.........++++++
writing new private key to '/etc/pki/tls/certs/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:cn
State or Province Name (full name) []:beijing
Locality Name (eg, city) [Default City]:beijing
Organization Name (eg, company) [Default Company Ltd]:NO
Organizational Unit Name (eg, section) []:beijing
Common Name (eg, your name or your server's hostname) []:www.jerryit.idv.cn
Email Address []:jerry@jerry.cn
[root@localhost certs]# chmod 600 vsftpd.pem   //将 Vsftpd 凭证设为不可以写入
```

## 配置SSL至Vsftpd配置文件

编辑vsftpd配置文件，配置凭证存放目录并开启SSL功能。

```
[root@localhost certs]# vi /etc/vsftpd/vsftpd.conf
rsa_cert_file=/etc/pki/tls/certs/vsftpd.pem    //凭证存放路径，根据凭证创建路径
ssl_enable=YES                                 //启动 SSL
force_local_data_ssl=YES                       //传输时强制使用 SSL
force_local_logins_ssl=YES                     //登录时强制使用 SSL
```

> **说明**
>
> 每行结尾不可以有空白，否则会发生错误。

配置完成后，必须重新启动vsftpd服务，这样配置值才会生效。

```
[root@localhost certs]# service vsftpd restart
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
```

## 连接测试

选择【文件】→【站点管理器】，单击【新站点】，输入主机IP地址，加密方式选择【要求



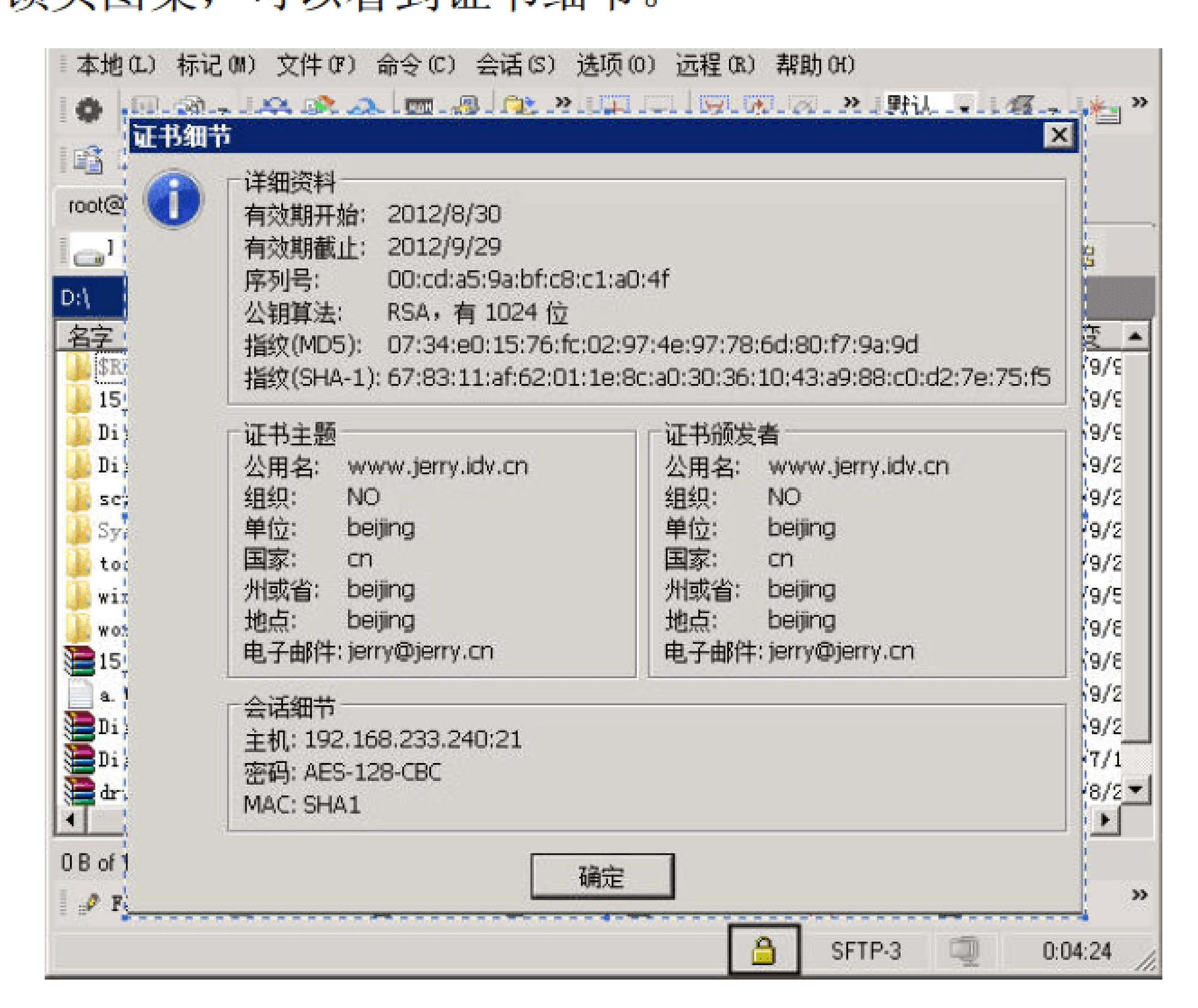
显示的FTP over TLS】，配置普通用户和密码，配置完成后，按【连接】进行测试。




成功连接后，会出现一个证书，确认无误后，按【确定】。




单击右下角的锁头图案，可以看到证书细节。



匿名用户可以用快速连接方式登录，一般用户必须用加密方式才可以正常登录。如果没有使用加密方式登录，会出现错误信息530 Non-anonymous sessions must use encryption。

```
响应:  220 Welcome to blah FTP service.
命令:  USER jerry
响应:  530 Non-anonymous sessions must use encryption.
错误:  无法连接到服务器
```

# 第9章

# BIND——名称解析服务器

BIND的全名是Berkeley Internet Name Domain，最初是由加州大学柏克莱分校开发出来的BSD UNIX中的一部分，目前则由ISC组织负责维护与开发。Bind服务用来提供域名与IP地址解析，并且是一个常用的DNS服务器软件，它提供了强大及稳定的名称解析服务，Linux系统上大多都以BIND软件作为DNS服务器，目前最新的版本为BIND 9.3.6。以下介绍怎样创建一个专用的DNS服务器。

## 9.1 安装Cache-only DNS服务器

Cache-only DNS服务器是DNS服务器的一部分，它本身并不管理任何域名，但是DNS客户端仍然可以向它请求查询。Cache-only DNS服务器类似于代理DNS服务器，它没有自己的查询数据库，而是将所有查询转发给其他DNS服务器进行查询，主要是为了加快DNS客户端的查询速度，当Cache-only服务器收到查询结果后，除了回应客户端外，还会将结果保存在缓存中。当下一个DNS客户端再查询相同的域名记录时，就可以从缓存里找出记录。为了提高客户端DNS的查询效率并减少局域网与广域网的流量，可以在局域网中创建一台Cache-only DNS服务器。配置Cache-only DNS服务器非常简单，只需要配置好named.conf配置文件即可。

### 安装BIND软件

在CentOS系统中BIND软件默认不安装，可以使用yum在线更新安装方法进行简单快速的安装，主要软件有bind、bind-chroot、bind-utils。

```
[root@localhost ~]# yum -y install bind bind-chroot bind-utils
Dependencies Resolved
======================================================================
 Package            Arch          Version                 Repository     Size
======================================================================
Installing:
 bind             x86_64     32:9.7.0-5.P2.el6_0.1        updates       3.5 M
```

```
 bind-chroot     x86_64     32:9.7.0-5.P2.el6_0.1       updates        65 k
Updating:
 bind-utils      x86_64     32:9.7.0-5.P2.el6_0.1       updates       174 k

Transaction Summary
========================================================================
Install       2 Package(s)
Upgrade       1 Package(s)

Total download size: 3.7 M
```

## 配置BIND服务

下面介绍如何配置DNS的Cache-only服务和DNS转发服务，用户根据自己的需求，可以配置多台DNS服务器，在配置文件中forwarders的选项要配置在options全局选项中，放到options全局选项外会发生错误。

```
[root@localhost /]# vi  /etc/named.conf
// named.conf
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver(as a localhost DNS resolver only).
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
        listen-on port 53 { any; };          //修改为 any，这样才可以对外连接
#       listen-on-v6 port 53 { ::1; };       //若没有使用 IPv6 协议，可以加上#
        directory       "/var/named";        //配置文件存放路径
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
                  //localhost 代表只有本机可以查询，要是对外提供服务，建议配置为 any
        recursion yes;
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";
        forward only;    //必须加上 forward only 否则 cache only 不会生效
        forwarders {
                      168.95.1.1;                       //配置转发服务器
                      8.8.8.8;
        };
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
```

```
};
zone "." IN {
        type hint;
        file "named.ca";
};
include "/etc/named.rfc1912.zones";
```

## 启动BIND服务器

配置完成后，就可以启动BIND服务器了，若有需要可将named服务设为系统默认启动。

```
[root@localhost /]# service named start
Starting named:                                              [  OK  ]
[root@localhost /]# chkconfig named on
```

## 配置防火墙

若要求BIND服务可以对外连接，必须在防火墙配置中开启TCP和UDP的53端口。

```
[root@localhost /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
                                                         //DNS TCP 53 Port
-A INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT
                                                         //DNS UDP 53 Port
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完毕后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost /]# service iptables restart
iptables: Flushing firewall rules:                           [  OK  ]
iptables: Setting chains to policy ACCEPT: filter            [  OK  ]
iptables: Unloading modules:                                 [  OK  ]
iptables: Applying firewall rules:                           [  OK  ]
```

## 测试BIND服务

利用dig命令查询www.google.com域名，使用BIND服务器本机IP地址127.0.0.1和BIND服务器对外IP地址192.168.233.200测试，查看是否可以正常解析。

```
[root@localhost /]#  dig www.google.com @127.0.0.1
                                                //BIND 服务器本机 IP 地址
; <<>> DiG 9.7.0-P2-RedHat-9.7.0-5.P2.el6_0.1 <<>> www.google.com @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41604
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.google.com.                        IN      A
;; ANSWER SECTION:
www.google.com.         558077  IN      CNAME   www.l.google.com.
www.l.google.com.       197     IN      A       74.125.31.99
www.l.google.com.       197     IN      A       74.125.31.103
www.l.google.com.       197     IN      A       74.125.31.104
www.l.google.com.       197     IN      A       74.125.31.105
www.l.google.com.       197     IN      A       74.125.31.106
www.l.google.com.       197     IN      A       74.125.31.147
;; Query time: 413 msec
;; SERVER: 127.0.0.1#53 (127.0.0.1)   //利用 127.0.0.1 可以查询到域名对应的 IP 地址代表解析成功
;; WHEN: Sun Aug 21 10:09:25 2011
;; MSG SIZE  rcvd: 148

[root@localhost /]#  dig www.google.com @192.168.233.200
                                                        //BIND 服务器对外 IP 地址
; <<>> DiG 9.7.0-P2-RedHat-9.7.0-5.P2.el6_0.1 <<>> www.google.com @192.168.233.200
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34376
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.google.com.                        IN     A
;; ANSWER SECTION:
www.google.com.         549189  IN      CNAME  www.l.google.com.
www.l.google.com.       189     IN      A      72.14.203.99
www.l.google.com.       189     IN      A      72.14.203.103
www.l.google.com.       189     IN      A      72.14.203.104
www.l.google.com.       189     IN      A      72.14.203.105
www.l.google.com.       189     IN      A      72.14.203.106
www.l.google.com.       189     IN      A      72.14.203.147
;; Query time: 298 msec
;; SERVER: 192.168.233.200#53 (192.168.233.200)
                                  /利用 192.168.233.200 可以查询到域名对应的 IP 地址代表解析成功
;; WHEN: Sun Aug 21 10:06:32 2011
;; MSG SIZE  rcvd: 148
```

使用dig测试时出现connection timed out; no servers could be reached错误信息。

```
[root@localhost /]#  dig www.google.com @127.0.0.1
; <<>> DiG 9.7.0-P2-RedHat-9.7.0-5.P2.el6_0.1 <<>> www.google.com @127.0.0.1
;; global options: +cmd
;; connection timed out; no servers could be reached
```

主要原因是配置文件named.conf内的listen-on port 53没有指定查询IP地址，所以无法查询。

```
[root@localhost /]# vi  /etc/named.conf
options {
        listen-on port 53 { 127.0.0.1;192.168.233.200; };
                             //默认为 127.0.0.1，若设为 any 代表接受任何 IP 地址
        listen-on-v6 port 53 { ::1; };
```

客户端利用BIND服务器查询时出现错误信息，原因在于allow-query选项。

```
> server 192.168.233.200
默认服务器:  [192.168.233.200]
Address:  192.168.233.200
> cn.yahoo.com
服务器:  [192.168.233.200]
Address:  192.168.233.200
*** [192.168.233.200] 找不到 cn.yahoo.com: Query refused
```

因为allow-query配置参数默认为localhost，所以无法对外查询，就算防火墙开启，用telnet也无法连通，所以必须配置为any，才可以正常查询。

```
[root@localhost /]# vi  /etc/named.conf
allow-query     { any; };              //默认为 localhost，设为 any 才可以对外查询。
```

# 9.2 配置BIND服务器

下面介绍如何利用DNS服务器实现域名和IP地址的正反向解析。

## 安装BIND软件

CentOS操作系统默认不会安装BIND软件，可以使用yum在线更新安装方法进行安装，主要软件有bind、bind-chroot、bind-utils。

```
[root@localhost ~]# yum  install  -y bind bind-chroot bind-utils
Dependencies Resolved
========================================================================
 Package            Arch         Version                  Repository    Size
========================================================================
Installing:
 bind             x86_64     32:9.7.0-5.P2.el6_0.1      updates       3.5 M
 bind-chroot      x86_64     32:9.7.0-5.P2.el6_0.1      updates        65 k
Updating:
 bind-utils       x86_64     32:9.7.0-5.P2.el6_0.1      updates       174 k
Transaction Summary
```

```
=========================================================================
Install        2 Package(s)
Upgrade        1 Package(s)
Total download size: 3.7 M
```

## 主要配置文件（named.conf）

Named.conf是Bind服务的主要配置文件，它管理所有根域的配置及Bind相关配置，以下示例配置域名的正反向解析。正反向解析名称可以根据需求配置，但是创建正反向解析文件时，文件名要一致，以免无法读取到正反向解析数据。

```
[root@localhost ~]# vi /etc/named.conf
// named.conf
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver(as a localhost DNS resolver only).
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
#       listen-on port 53 { any; };      //修改为 any，这样才可以对外连接
#       listen-on-v6 port 53 { none; };
                               //与上一行作用相同，若不使用 IPv6 协议则加上#号
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
                             // 允许客户端查询范围，配置为 any 开放所有 IP 都可以查询
        recursion yes;
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;
        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
        zone "." IN {                                //根服务配置文件
                type hint;
                file "named.ca";
        };
        zone "jerryit.idv.cn" IN {                   //正向解析配置
                type master;                         //服务器类型
```

```
                file "jerryit.idv.cn";                  //正向解析文件名
                allow-update { none; };
        };
        zone "0.168.192.in-addr.arpa" IN {              //反向解析配置
                type master;
                file "192.168.233";                     //反向解析文件名
                allow-update { none; };
        };
include "/etc/named.rfc1912.zones";
```

## 配置根服务器文件

此文件为根服务器地址的配置文件，在DNS服务器的名称解析中，如果DNS服务器的数据库没有包含所要求查询的记录，则此服务器首先会要求根服务器解析有关域名的类型。最新信息可以到ftp://rs.internic.net/domain 下载。

```
[root@localhost ~]# vi /var/named/named.ca
; <<>> DiG 9.5.0b2 <<>> +bufsize=1200 +norec NS . @a.root-servers.net
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34420
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 20
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS
;; ANSWER SECTION:
.                       518400  IN      NS      M.ROOT-SERVERS.NET.
.                       518400  IN      NS      A.ROOT-SERVERS.NET.
.                       518400  IN      NS      B.ROOT-SERVERS.NET.
.                       518400  IN      NS      C.ROOT-SERVERS.NET.
.                       518400  IN      NS      D.ROOT-SERVERS.NET.
.                       518400  IN      NS      E.ROOT-SERVERS.NET.
.                       518400  IN      NS      F.ROOT-SERVERS.NET.
.                       518400  IN      NS      G.ROOT-SERVERS.NET.
.                       518400  IN      NS      H.ROOT-SERVERS.NET.
.                       518400  IN      NS      I.ROOT-SERVERS.NET.
.                       518400  IN      NS      J.ROOT-SERVERS.NET.
.                       518400  IN      NS      K.ROOT-SERVERS.NET.
.                       518400  IN      NS      L.ROOT-SERVERS.NET.
;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     3600000 IN      A       198.41.0.4
A.ROOT-SERVERS.NET.     3600000 IN      AAAA    2001:503:ba3e::2:30
B.ROOT-SERVERS.NET.     3600000 IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     3600000 IN      A       192.33.4.12
D.ROOT-SERVERS.NET.     3600000 IN      A       128.8.10.90
E.ROOT-SERVERS.NET.     3600000 IN      A       192.203.230.10
F.ROOT-SERVERS.NET.     3600000 IN      A       192.5.5.241
```

```
F.ROOT-SERVERS.NET.    3600000 IN      AAAA    2001:500:2f::f
G.ROOT-SERVERS.NET.    3600000 IN      A       192.112.36.4
H.ROOT-SERVERS.NET.    3600000 IN      A       128.63.2.53
H.ROOT-SERVERS.NET.    3600000 IN      AAAA    2001:500:1::803f:235
I.ROOT-SERVERS.NET.    3600000 IN      A       192.36.148.17
J.ROOT-SERVERS.NET.    3600000 IN      A       192.58.128.30
J.ROOT-SERVERS.NET.    3600000 IN      AAAA    2001:503:c27::2:30
K.ROOT-SERVERS.NET.    3600000 IN      A       193.0.14.129
K.ROOT-SERVERS.NET.    3600000 IN      AAAA    2001:7fd::1
L.ROOT-SERVERS.NET.    3600000 IN      A       199.7.83.42
M.ROOT-SERVERS.NET.    3600000 IN      A       202.12.27.33
M.ROOT-SERVERS.NET.    3600000 IN      AAAA    2001:dc3::35
;; Query time: 147 msec
;; SERVER: 198.41.0.4#53 (198.41.0.4)
;; WHEN: Mon Feb 18 13:29:18 2008
```

## 配置域名正向解析文件

主要文件配置完毕后，就可以开始创建正向解析文件了，这里配置A、MX、CNAME类型。

| 名称 | 类型 | 优先等级 | 对应信息 |
|---|---|---|---|
| bind | A | | 192.168.233.200 |
| mailsrv | A | | 192.168.233.150 |
| @ | MX | 10 | mailsrv.jerryit.idv.cn |
| www | CNAME | | bind.jerryit.idv.cn |

在named目录下创建正向解析文件，正向解析文件的名称必须要与主配置文件内的配置相同，否则无法读取。先配置SOA信息，然后再配置其他信息。

```
[root@localhost ~]# vi /var/named/jerryit.idv.cn   //创建并编辑正向解析文件

$TTL 86400
@   IN  SOA     bind.jerryit.idv.cn. root.jerryit.idv.cn. (
                                                            //管理 BIND 服务器管理信息
        2011071001     ;序号 Serial
        3600           ;更新频率 Refresh
        1800           ;失败重新尝试时间 Retry
        604800         ;失效时间 Expire
        86400          ;快取时间 Minimum TTL
)
        IN  NS            bind.jerryit.idv.cn. //BIND 服务器主机
        IN  A             191.168.233.200      //BIND 服务器 IP 地址
        IN  MX 10      mailsrv.jerryit.idv.cn. //邮件服务器
bind   IN  A           192.168.233.200      //网络域名 IP 地址
mailsrv IN  A          192.168.233.150
www      IN CNAME      bind.jerryit.idv.cn.            //网域主机的第二名称
```

## 配置域名反向解析文件

正向解析文件配置完毕后，接下来创建反向解析文件，反向解析文件很简单，类型也只有PTR记录，PTR记录的信息就是正向解析文件内的类型A主机的IP地址。

| 名称 | 类型 | 对应信息 |
|---|---|---|
| 200 | PTR | bind.jerryit.idv.cn |
| 150 | PTR | mail.jerryit.idv.cn |

在named目录下创建反向解析文件，反向解析文件的名称必须要与主要配置文件内的配置相同，否则无法正常读取，先配置SOA信息，然后再配置其他信息。

```
[root@localhost ~]# vi /var/named/192.168.233 //创建并编辑反向解析档
$TTL 86400
@   IN  SOA    bind.jerryit.idv.cn. root.jerryit.idv.cn. (
                                              //管理 BIND 服务器管理信息
        2011071001  ;序号 Serial
        3600        ;更新频率 Refresh
        1800        ;失败重新尝试时间 Retry
        604800      ;失效时间 Expire
        86400       ;快取时间 Minimum TTL
)
        IN  NS     bind.jerryit.idv.cn.   //NS 服务器主机名
        IN  PTR    jerryit.idv.cn.
        IN  A      255.255.255.0
200     IN  PTR    bind.jerryit.idv.cn.   //反向解析查询 IP 主机
150     IN  PTR    mailsrv.jerryit.idv.cn
```

## 启动BIND服务器

配置完成后，就可以启动BIND服务了，若有需要将named服务设为系统默认启动。

```
 [root@localhost /]# service named start
Starting named:                                            [  OK  ]
[root@localhost /]# chkconfig named on
```

## 配置防火墙

若要求BIND服务可以对外连接，必须在防火墙配置中开启TCP和UDP的53端口。

```
 [root@localhost /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
                                                        //DNS TCP 53 Port
-A INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT
                                                        //DNS UDP 53 Port
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完毕后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost /]# service iptables restart
iptables:Flushing firewall rules:                          [  OK  ]
iptables:Setting chains to policy ACCEPT: filter           [  OK  ]
iptables:Unloading modules:                                [  OK  ]
iptables:Applying firewall rules:                          [  OK  ]
```

## 测试BIND 服务

在客户端计算机上使用nslookup测试BIND服务器，输入【nslookup】，默认会使用客户端配置的DNS服务器, 所以必须修改成刚创建的DNS服务器IP地址, 输入【server 192.168.233.200】

首先进行正向解析查询，检查正向解析文件内的A类型，如果都可以正常查询，则代表配置成功。

```
> bind.jerryit.idv.cn
服务器:[192.168.233.200]
Address:192.168.233.200
名称:bind.jerryit.idv.cn
Address:192.168.233.200
> mailsrv.jerryit.idv.cn
服务器:[192.168.233.200]
Address:192.168.233.200
名称:mailsrv.jerryit.idv.cn
Address:192.168.233.150
```

其次测试MX类型，建议将条件配置为只查询类型MX，然后再查询，如果可以查询出mail exchanger所配置的IP地址，代表配置成功。

```
> set q=mx                                              //配置为只查询 MX 类型
> jerryit.idv.cn                                        //输入域名
服务器:[192.168.233.200]
Address:192.168.233.200
jerryit.idv.cn  MX preference = 10, mail exchanger = mailsrv.jerryit.idv.cn
jerryit.idv.cn  nameserver = bind.jerryit.idv.cn
bind.jerryit.idv.cn     internet address = 192.168.233.200
```

再测试CNAME类型，如果查询到别名主机所配置的IP地址，代表配置成功。

```
> www.jerryit.idv.cn
服务器:[192.168.233.200]
Address:192.168.233.200
www.jerryit.idv.cn      canonical name = bind.jerryit.idv.cn
jerryit.idv.cn
        primary name server = bind.jerryit.idv.cn
        responsible mail addr = root.jerryit.idv.cn
        serial  = 2011071001
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
```

最后测试反向解析，输入配置文件内的PTR类型，若能够查询到主机名，代表解析成功。

```
> 192.168.233.200
服务器:[192.168.233.200]
Address:192.168.233.200
名称:bind.jerryit.idv.cn
Address:192.168.233.200
> 192.168.233.150
服务器:[192.168.233.200]
Address:192.168.233.200
名称:mail.jerryit.idv.cn
Address:192.168.233.150
```

# 第10章

# Samba——文件服务器

Samba是一种开放源代码软件，用来让UNIX系列的操作系统与微软Windows操作系统的SMB/CIFS（Server Message Block/Common Internet File System）网络协议的资源共享之间实现相互访问。不仅可读取及共享SMB的目录及打印机，本身还可以加入Windows Server的网络、扮演为域控制器（Domain Controller）以及成为Active Directory成员。简而言之，此软件在Windows与UNIX系列OS之间搭起一座桥梁，让两者可互通有无，目前的版本为v3。

## 10.1 安装Samba服务

下面介绍如何安装Samba服务，并配置一个公共的共享目录。

### 检查Samba软件

安装Samba服务前，先检查Samba软件，确认是否已安装samba、samba-client、samba-common软件，若有代表已经安装过。

```
[root@localhost ~]# rpm -qa | grep samba
samba-winbind-clients-3.5.4-68.el6_0.2.x86_64
samba-common-3.5.4-68.el6_0.2.x86_64
samba-client-3.5.4-68.el6_0.2.x86_64
samba-3.5.4-68.el6_0.2.x86_64
```

### 安装Samba软件

安装Samba软件，建议使用yum在线更新方法进行安装，较方便快速。

```
[root@localhost ~]# yum install -y samba
Dependencies Resolved
========================================================================
```

```
 Package                    Arch         Version            Repository    Size
========================================================================
Installing:
 samba                     x86_64     3.5.4-68.el6_0.2      updates      5.0 M
Updating for dependencies:
 samba-client              x86_64     3.5.4-68.el6_0.2      updates       11 M
 samba-common              x86_64     3.5.468.el6_0.2       updates       13 M
 samba-winbind-clients     x86_64     3.5.4-68.el6_0.2      updates      1.1 M

Transaction Summary
========================================================================
Install       1 Package(s)
Upgrade       3 Package(s)

Total download size: 30 M
```

## 创建Samba共享目录

Samba软件安装完毕后，创建一个共享目录，此共享目录名称为test，先在根目录创建名称为test的目录，将test目录权限修改为nobody，使每个人都可以使用。

```
[root@localhost ~]# mkdir /test      //创建 test 共享目录
[root@localhost ~]# chown  nobody  /test   //配置共享目录权限
```

## 配置Samba 服务

接下来编辑Samba配置文件，首先编辑工作组，默认为MYGROUP，这里使用默认的Samba工作组，若没有配置也不影响使用，只是在使用工作组去搜索共享目录时会找不到。

```
[root@localhost ~]# vi /etc/samba/smb.conf
        workgroup = MYGROUP          //默认为 MYGROUP，可根据实际环境配置
        server string = Samba Server Version %v
```

使用Samba共享目录就必须输入账号和密码，要让用户登录Samba共享目录时不用输入密码，就必须将user改成share。安全性等级默认为user。

```
[root@localhost ~]# vi /etc/samba/smb.conf
      security = share     //默认为 user，需要输入账号和密码才可以登录，若要共享则设为 share
      passdb backend = tdbsam
```

指定Samba是否是本地主浏览器，默认值是yes。如果设为no，则Samba服务器永远都不会成为本地主浏览器。如果配置文件中没有启用，将【;】号删除，并把no改成yes。

```
[root@localhost ~]# vi /etc/samba/smb.conf
       local master = yes
```

配置共享目录，在Samba配置文件的最后一行创建Samba共享目录信息。

```
[root@localhost ~]# vi /etc/samba/smb.conf
       [test]
       comment = test          //配置共享目录名称
       path = /test            //配置共享目录路径
       read only = no          //是否只有读取权限
       guest ok = yes          //是否可以使用访客账号登录
       browseable = yes        //是否可以浏览目录内容
```

## 检查配置文件

测试Samba配置文件是否正确，如果看到test正常显示，表示配置成功。

```
[root@localhost ~]# testparm          //检查 Samba 配置文件
Load smb config files from /etc/samba/smb.conf
rlimit_max: rlimit_max (1024) below minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[test]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions  //按 Enter

[global]
        workgroup = MYGROUP
        server string = Samba Server Version %v
        log file = /var/log/samba/log.%m
        max log size = 50
        cups options = raw

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

[test]                         //范例中创建的共享目录
        comment = test
        path = /test
        write list = +staff
        read only = No
        guest ok = Yes
```

## 启动Samba

Samba配置完成后，就可以启动Samba服务了，若Samba提供对外服务，就需要将Samba服务设为系统默认启动。

```
[root@localhost ~]# service smb start
Starting SMB services:                                     [  OK  ]
[root@localhost ~]# chkconfig smb on
```

## 配置防火墙

使用Samba服务前，必须在防火墙配置文件中开启Samba所需的端口，Samba使用的端口为137、138、139、445，这样才可以对外连接。

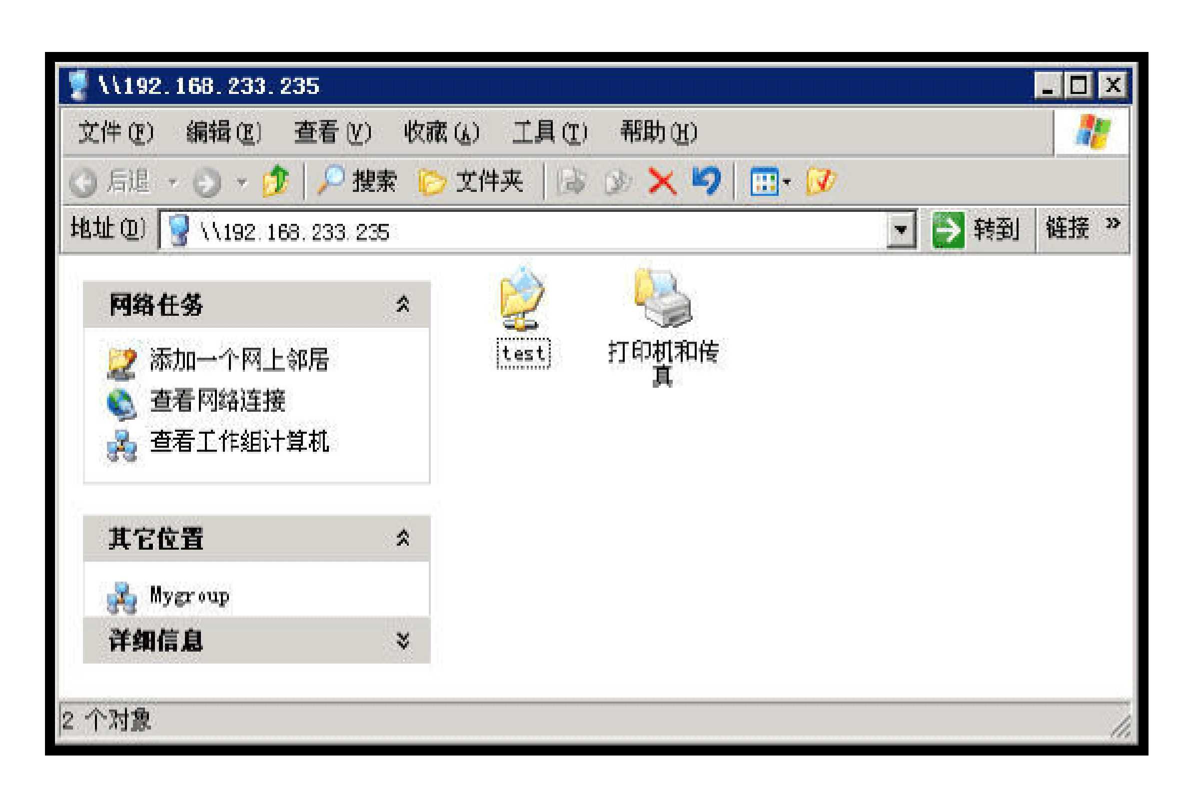
```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 137 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 138 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
~
```

防火墙配置完毕后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

## 测试Samba共享目录

启动成功后，在Windows客户端执行【开始】→【运行】，输入【\\IP地址】，即会看到共享的目录test及共享的打印机。




若共享目录配置正确，又出现下面的错误信息，则是SELinux安全性造成的。




检查发现SELinux状态为开启，建议关闭，防止测试中出现错误信息。

```
[root@localhost ~]# vi /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled                  //默认为 enforcing 开启，若关闭则设为 disabled
```

若出现状态无法保存或无法创建新文件的情况，如下图所示。




原因在于Samba配置文件内配置了read only = yes，所以只能浏览，设为no或删除就可以保存和创建新文件了。

```
[root@localhost ~]# vi /etc/samba/smb.conf
       [test]
       comment = test
```

```
        path = /test
        read only = yes                    //  设为 yes 只能读取，无法修改或新增
        guest ok = yes
        browseable = yes
```

# 10.2 配置USER等级共享目录

Samba服务器已经介绍过share等级的配置，不用输入密码，就可以使用Samba共享目录，以下介绍user等级配置，此等级必须要输入账号和密码才可以使用，不像share等级可以随意登录，这样可以提高服务器的安全性。

## 配置共享权限

编辑Samba配置文件，安全性等级默认为user，若要使用Samba共享目录就必须输入账号和密码。

```
[root@localhost ~]# vi /etc/samba/smb.conf
      security = user      //默认为 user，需要输入主机账号才可以登录，共享则设为 share
      passdb backend = tdbsam
```

指定Samba是否是本地主浏览器，默认值是yes。如果设为no，则Samba服务器永远都不会成为本地主浏览器。如果配置文件中没有启用，将【;】号删除。

```
 [root@localhost ~]# vi /etc/samba/smb.conf
       local master = yes
```

## 管理账号和密码

Samba 2 版本以前的用户账号管理是使用smbpasswd，密码文件为文本文件，用户比较多的情况下，效率较差。Samba 3 版本的用户账号管理默认使用后端 tdbsam 数据库管理机制，目前版本以Samba 3为主。

| 命令参数 | 命令说明 |
|---|---|
| pdbedit -L | 列出 samba 用户列表 |
| pdbedit -Lv | 列出详细的 samba 用户列表 |
| pdbedit -Lw | 列出同 smbpasswd 格式的用户列表 |
| pdbedit -a jerry | 新增 jerry 用户 |
| pdbedit -x jerry | 删除 jerry 用户 |
| pdbedit -c "[D]" -u jerry | 暂时停用 jerry 这个用户 |
| pdbedit -c "[]" -u jerry | 恢复使用 jerry 这个用户 |

首先创建一个Samba服务使用的账号jerry，并允许登录，前提是home目录内有jerry用户的主目录。

```
[root@localhost ~]# pdbedit  -a  jerry  //创建一个 samba 用户 jerry
new password:
retype new password:
Unix username:         jerry
NT username:
Account Flags:         [U          ]
User SID:              S-1-5-21-771671275-2027446412-3136032341-1000
Primary Group SID:     S-1-5-21-771671275-2027446412-3136032341-513
Full Name:
Home Directory:        \\myserver\jerry
HomeDir Drive:
Logon Script:
Profile Path:          \\myserver\jerry\profile
Domain:                MYSERVER
Account desc:
Workstations:
Munged dial:
Logon time:            0
Logoff time:           9223372036854775807 seconds since the Epoch
Kickoff time:          9223372036854775807 seconds since the Epoch
Password last set:     Tue, 23 Aug 2011 01:54:05 CST
Password can change:   Tue, 23 Aug 2011 01:54:05 CST
Password must change: never
Last bad password    : 0
Bad password count   : 0
Logon hours          : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

若本机home目录下没有要指定的samba用户名称，则无法添加新用户，例如long，本机没有这个账号，所以就无法新增成功，所以必须要新增本机账号，再新增samba账号。

```
[root@localhost jerry]# pdbedit  -a  long
new password:
retype new password:
Failed to add entry for user long.
```

## 启动Samba服务

Samba配置完成后，就可以启动Samba服务了，若Samba提供对外服务，那就需要将Samba服务设为系统默认启动。

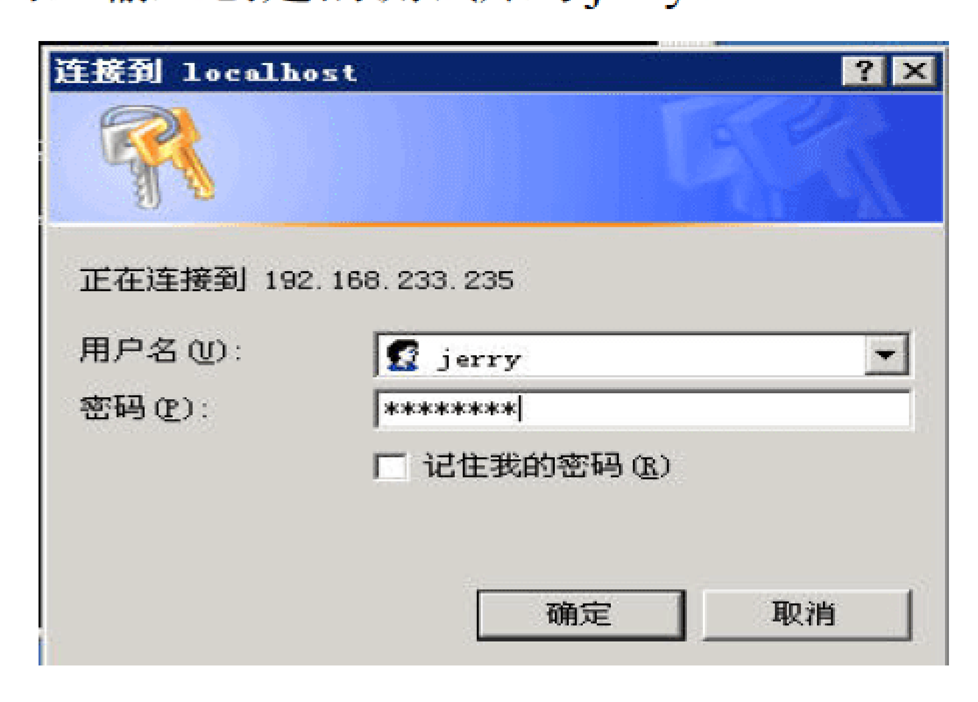
```
[root@localhost ~]# service smb start
Starting SMB services:                                     [  OK  ]
[root@localhost ~]# chkconfig smb on
```

**说明**

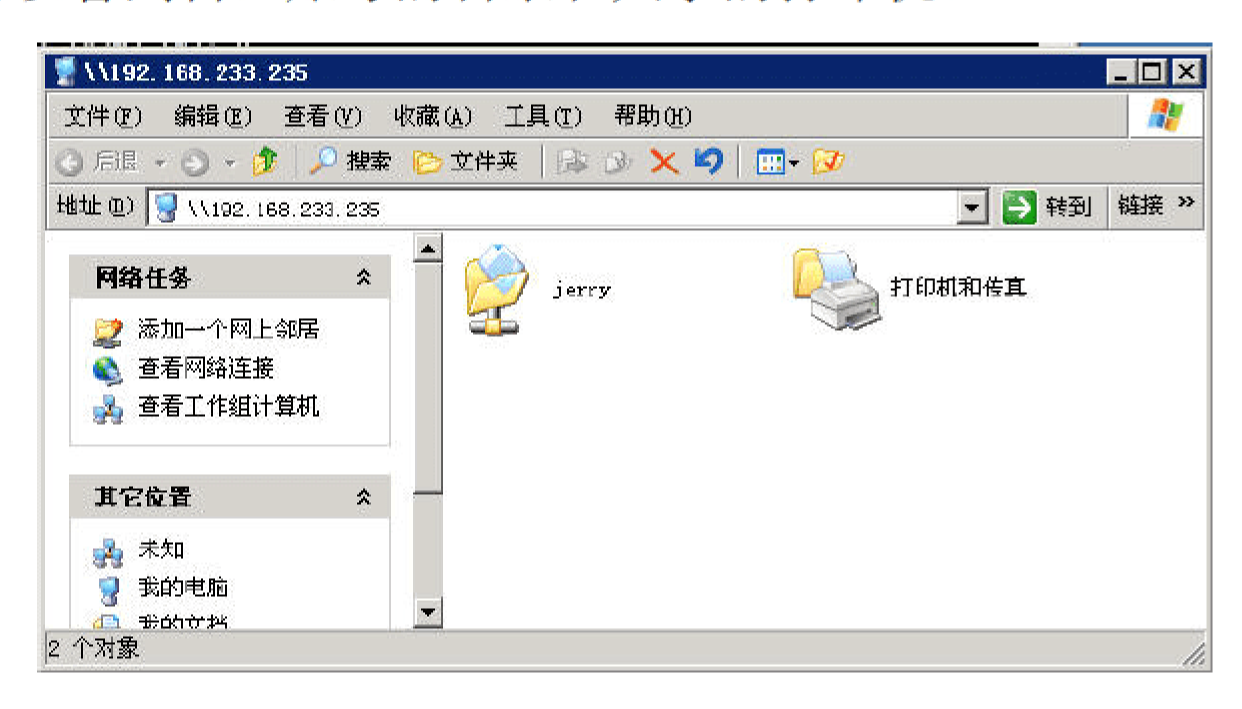
记得在防火墙配置文件中开启端口137、138、139、445。

## 测试USER等级的目录

在Windows客户端检查是否可以正常登录。输入用户名和密码后，输入【\\IP地址】，如下图所示，需要输入用户密码，输入创建的测试账号jerry。




正常登录后，可以看到自己账号的目录和共享的打印机。




## 10.3 SWAT-Samba WEB管理工具

SWAT（Samba WEB Administration Tool）是Samba的图形化管理工具，可以通过浏览器使用SWAT工具来设置Samba。在SWAT中每一个Samba参数都有对应的帮助文件或解释文件，很适合初学者使用。

## 安装SWAT工具

安装SWAT工具，建议使用yum在线更新方式进行安装，既方便又快速。

```
[root@localhost]# yum install  -y samba-swat        //安装 SWAT
Dependencies Resolved
==================================================================
 Package            Arch          Version        Repository       Size
==================================================================
Installing:
```

```
 samba-swat       x86_64      3.5.4-68.el6_0.2       updates         3.0 M
Installing for dependencies:
 xinetd          x86_64      2:2.3.14-29.el6         base            120 k
Transaction Summary
========================================================================
Install       2 Package(s)
Upgrade       0 Package(s)
Total download size: 3.2 M
```

## 配置SWAT

编辑SWAT配置文件，在only_from前面添加注解符[#]，不然只允许本机可以连接，将disable配置为no，这样才可以启动SWAT。

```
[root@localhost ~]# vi /etc/xinetd.d/swat
# default: off
# description: SWAT is the Samba Web Admin Tool. Use swat \
#              to configure your Samba server. To use SWAT, \
#              connect to port 901 with your favorite web browser.
service swat
{
        port            = 901
        socket_type     = stream
        wait            = no
#       only_from       = 127.0.0.1            //若不加上#号则只允许本机连接
        user            = root
        server          = /usr/sbin/swat
        log_on_failure += USERID
        disable         = no                   //默认为 yes 不可以使用，需配置为 no 才可以使用
```

## 启动SWAT

SWAT配置完成后，就可以启动SWAT了，若经常使用需将SWAT设为默认启动。

```
[root@localhost ~]# service xinetd start
Starting xinetd:                                          [  OK  ]
[root@localhost ~]# chkconfig xinetd on
```

## 配置防火墙

SWAT使用的端口为901，需在防火墙中开启，这样服务才可以对外连接。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
```

```
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 901 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完毕后，必须重新启动服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                     [  OK  ]
iptables: Setting chains to policy ACCEPT: filter      [  OK  ]
iptables: Unloading modules:                           [  OK  ]
iptables: Applying firewall rules:                     [  OK  ]
```

## 使用SWAT

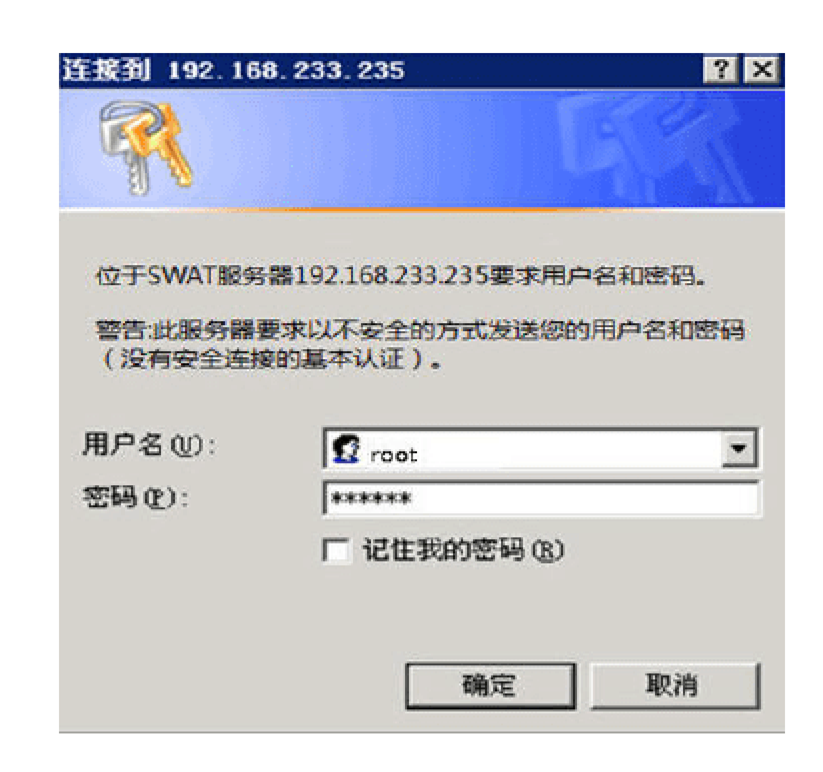
打开浏览器，输入【http://IP地址：901】，先使用普通用户登录，查看是否与管理员账号有差别。



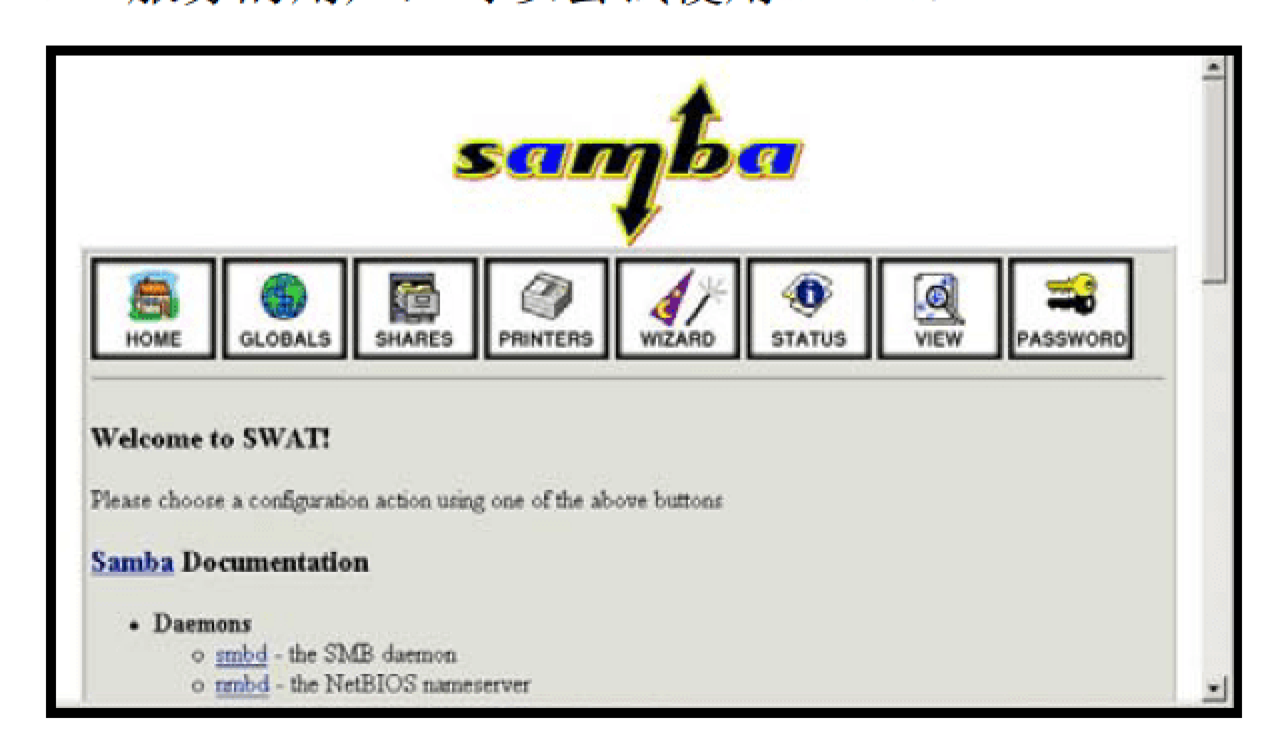

使用普通用户登录只会有下列4种管理界面，没有完整的管理功能，基本上只有查看功能。




再来以root管理员用户登录，检查管理功能是否有差别。




以root管理员用户登录后，SWAT多了很多管理功能，可以查看共享目录，并且可以进行配置，不太会使用Samba服务的用户，可以尝试使用SWAT。



# 第 11 章

# Squid（Proxy）——代理服务器

Proxy的意思是代理软件或代理服务器，其功能主要是接受用户的请求后，替用户连至Internet上读取网页数据，然后将数据保存于硬盘中，再将数据传送给用户。当有其他用户要求读取同一份数据时，Proxy Server便可将存放于硬盘上的数据传送给用户，借此可减少重复的数据获取，节省不必要的数据传输，进一步降低网络的负载。Squid是Linux常见的Proxy服务，配置简单又好管理。

## 11.1 Squid的安装和配置

Squid安装方式很简单，以下介绍如何配置一个简单的Proxy代理服务器，以供公司内部使用。

### 安装Squid

如果要使用squid服务，必须安装软件Squid和perl-URI，建议使用yum在线更新方式进行安装，既简单又方便。

```
[root@localhost /]# yum -y install squid
Dependencies Resolved

========================================================================
 Package           Arch            Version              Repository      Size
========================================================================
Installing:
 squid          x86_64       7:3.1.10-1.el6             base         1.7 M

Transaction Summary
========================================================================
Install        1 Package(s)
Upgrade        0 Package(s)
```

```
Total download size: 1.7 M
```

安装完成后，启动前必须要编辑squid配置文件，默认端口为3128，常见的Proxy代理服务器软件默认端口都是3128，建议进行修改，尽量是较少人使用的端口，这样被扫描到的机率会较小，以降低使用的效率与带宽。

```
[root@localhost /]# vi /etc/squid/squid.conf
# Squid normally listens to port 3128
http_port 3128          //端口 3128，CentOS 6.0 默认启用，之前的版本需要将#号移除
```

## 配置防火墙

Squid代理服务器配置完成后，启动前必须要在防火墙中开启squid代理服务器端口3128，以免无法对外使用。

```
[root@localhost /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 3128 -j ACCEPT
                                                            //squid 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

配置完防火墙后，必须要重新启动防火墙，配置才会生效。

```
[root@localhost /]# service iptables restart
iptables: Flushing firewall rules:                        [  OK  ]
iptables: Setting chains to policy ACCEPT: filter         [  OK  ]
iptables: Unloading modules:                              [  OK  ]
iptables: Applying firewall rules:                        [  OK  ]
iptables: Loading additional modules: nf_conntrack_ftp    [  OK  ]
```

## 启动squid代理服务器

简单的squid代理服务器配置完成后，就可以启动squid了，如果该服务经常使用，建议配置为系统默认启动，这样重新启动系统后就会自动启动该服务，避免忘记启动而导致无法使用。

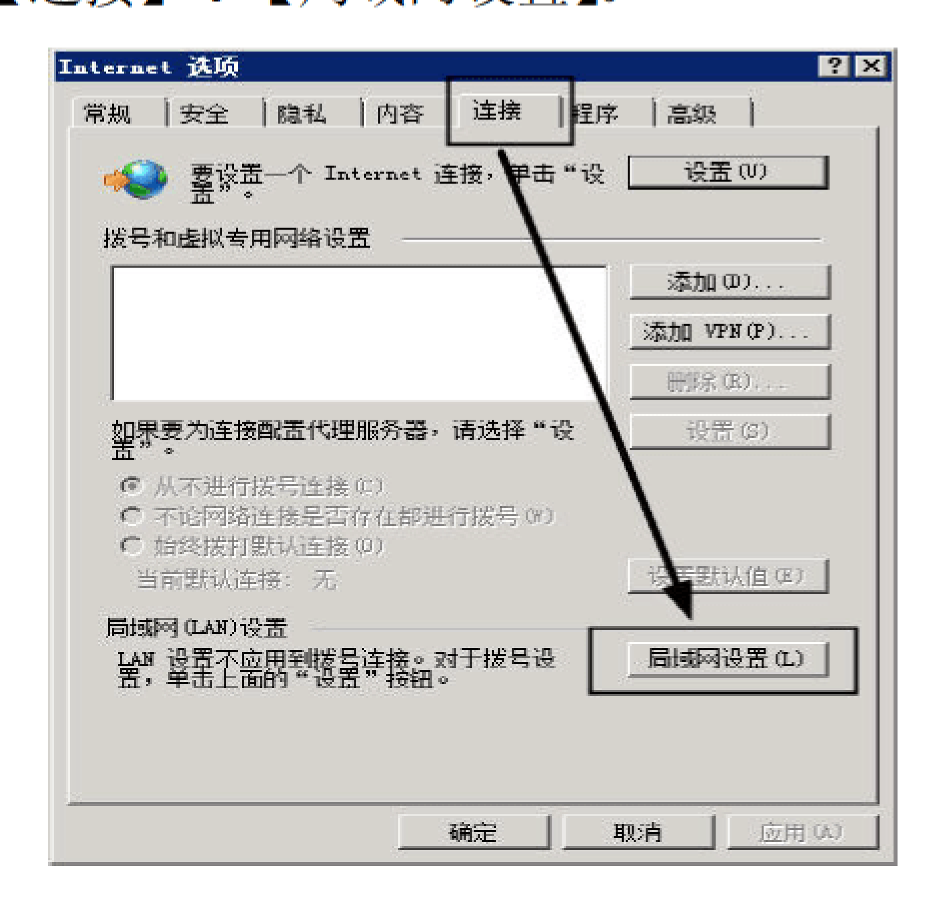
```
[root@localhost /]# service squid start
Starting squid: .                                          [  OK  ]
```

成功启动squid代理服务器后，检查端口3128是否正常开启。

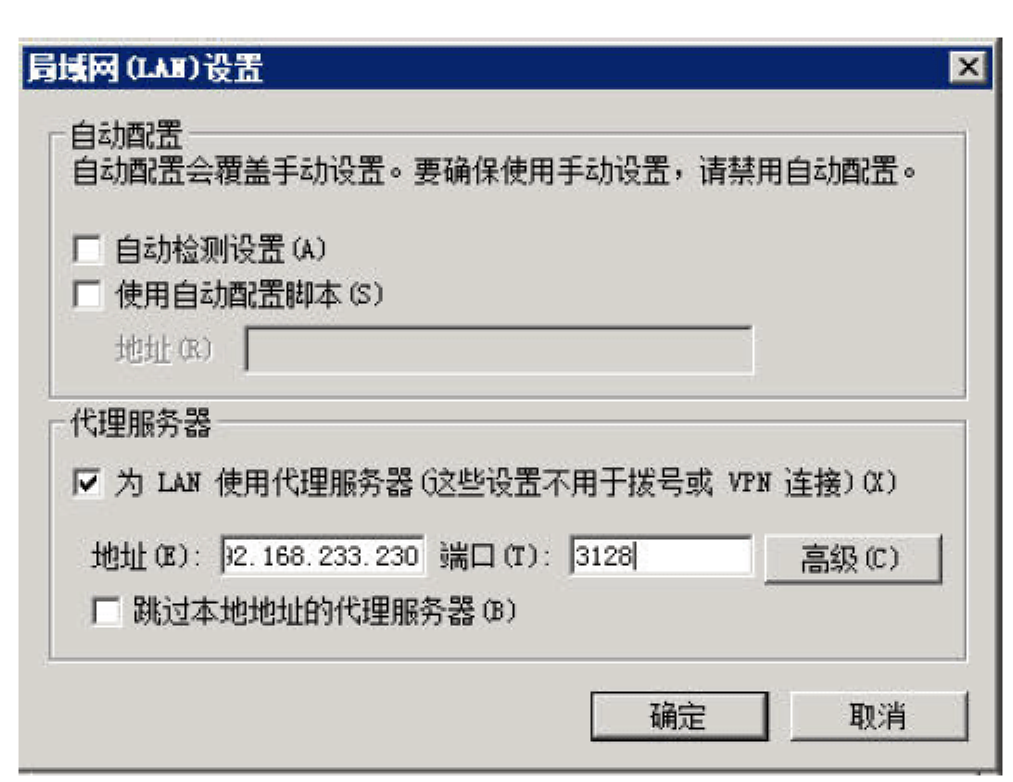
```
[root@localhost /]# netstat -tunlp | grep squid
tcp        0      0 :::3128                     :::*                        LISTEN      3127/(squid)
udp        0      0 :::52051                    :::*                                    3127/(squid)
```

## 客户端使用squid代理服务器

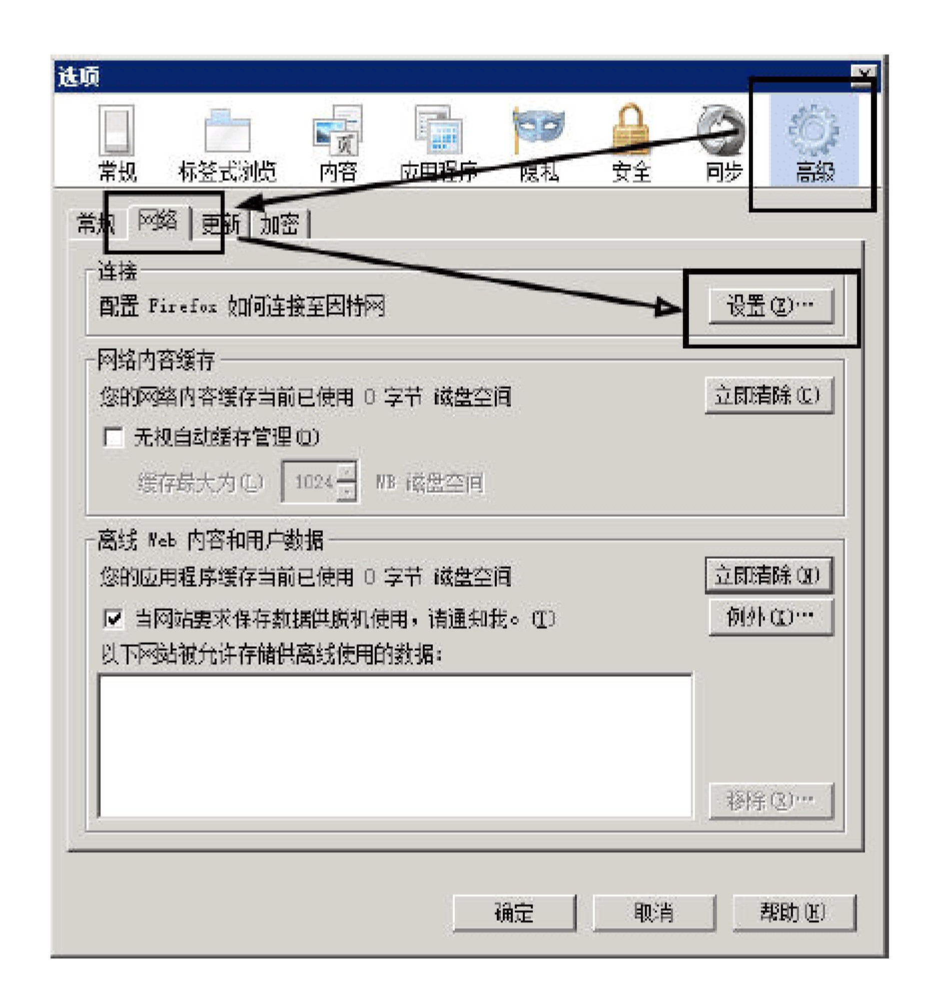
使用Windows客户端，设置Internet Explorer（IE）浏览器使用Proxy服务器的方法如下，【工具】→【Internet选项】→【连接】→【局域网设置】。



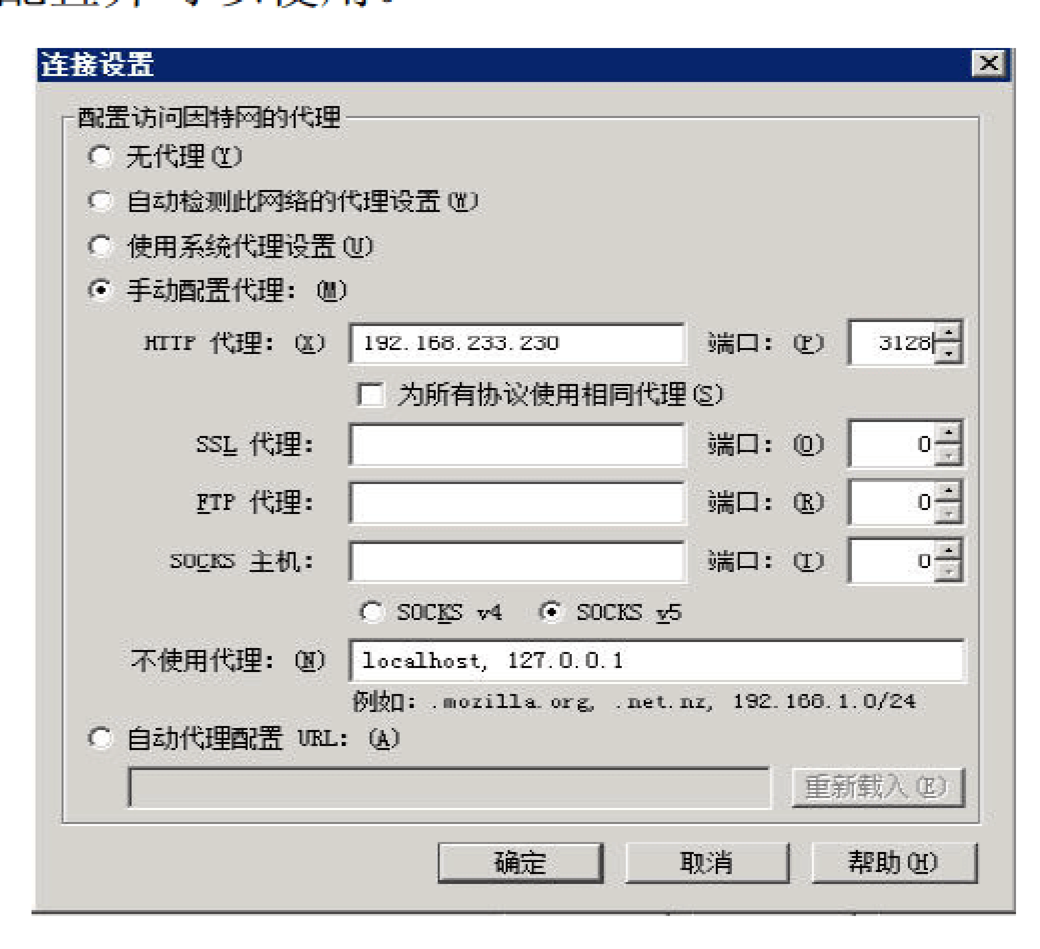

在代理服务器中勾选【为LAN使用代理服务器（这些设置不用于拨号或VPN连接）】，输入代理服务器的IP地址，和端口号3128，按下【确定】，即完成配置并可以使用。




设置Firefox浏览器使用Proxy服务器的方法，【选项】→【高级】→【网络】→【设置】。




选择【手动配置代理】，在HTTP 代理中配置代理服务器的IP地址和端口3128，配置完成后，按【确定】，即完成配置并可以使用。




打开浏览器后，输入网址即可以正常浏览网页。



# 11.2 配置Squid缓存目录

Squid代理服务器的cache缓存目录可以说是squid的硬盘，每当用户要求连接到一个网站时，squid代理服务器会先到cache缓存目录中检查是否有相同的数据，如果有相同的数据就不会到网络去下载，而是直接将缓存数据提供给用户。举例来说，同一时间有3位用户要连接到yahoo，第一位用户连接时，squid查询cache缓存目录内没有数据，squid代理服务器会主动去yahoo下载一份网页数据，当第二位用户要连接yahoo时，cache缓存目录已存在一份网页数据，squid代理服务器就将cache缓存目录内的网页提供给第二位用户，然后第三位用户连接时，虽然cache中有一份网页数据，但是Squid代理服务器发现网页内容已更新，squid代理服务器就会自动再下载一份最新的网页到cache缓存目录内，这就是cache的好处。

当用户请求网页数据时，代理服务器所获取的网页数据会存放到缓存目录内，所以缓存目录的大小，会影响squid代理服务器的运行，所以有效地配置缓存目录大小非常重要。

## 开启Squid缓存目录

要修改squid代理服务器的缓存目录，必须要编辑squid配置文件，将cache_dir一行前面的【#】号删除，才可以指定squid缓存目录的路径和缓存文件大小，缓存目录默认路径为/var/spool/squid，默认容量上限为100MB，可以按需求修改，不过建议不要将容量修改得过大，以免影响服务器效率。

```
[root@localhost /]# vi /etc/squid/squid.conf
# Uncomment and adjust the following to add a disk cache directory.
cache_dir ufs /var/spool/squid 100 16 256          //默认不启用，移除#号则启用
```

成功配置缓存目录后，必须重新启动squid代理服务器，配置才会生效，重新启动的时间有时会比较长，cache文件越大，启动速度越慢。

```
[root@localhost squid]# service squid restart
Stopping squid: 2012/08/23 07:50:44| WARNING cache_mem is larger than total disk cache
space!
................                                          [  OK  ]
init_cache_dir /var/spool/squid... Starting squid: .      [  OK  ]
```

CentOS 6.x操作系统在安装squid后，cache缓存目录大小默认为100MB，当启动时会警告要求使用更大的容量，不用理会这个警告，代理服务器还可以正常运行，以前版本配置100MB是不会有任何警告的，可以输入命令或重新启动服务检查是否需要加大。

```
[root@localhost squid]# service squid status
squid (pid  4311) is running...
2012/08/23 09:39:39| WARNING cache_mem is larger than total disk cache space!
```

将目录切换到cache缓存目录下，检查cache缓存目录名称squid，查看squid缓存目录的属性，发现拥有者及群组都是squid。

```
[root@localhost /]# cd /var/spool
```

```
[root@localhost spool]# ll
total 40
drwxr-xr-x.  2 abrt    abrt   4096 Nov 12  2010 abrt
drwx------.  2 abrt    abrt   4096 Nov 12  2010 abrt-upload
drwxr-xr-x.  2 root    root   4096 Aug 19  07:09 anacron
drwx------.  3 daemon  daemon 4096 Aug 19  07:08 at
drwx------.  2 root    root   4096 Nov 11  2010 cron
drwxr-xr-x.  2 root    root   4096 Nov 11  2010 lpd
drwxrwxr-x.  2 root    mail   4096 Aug 20  10:18 mail
drwxr-xr-x.  2 root    root   4096 Aug 23  05:22 plymouth
drwxr-xr-x. 16 root    root   4096 Aug 19  07:09 postfix
drwxr-x---.  2 squid   squid  4096 Aug 23  2012 squid //squid cache 默认目录
```

接下来进入squid缓存目录，查看缓存目录内的所有文件，有一个文件名为swap.state，swap.state文件的大小会随浏览网页的增多而增加。

```
[root@localhost /]# cd /var/spool/squid           //进入 squid 默认缓存目录
[root@localhost squid]# ll
total 72
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 00
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 01
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 02
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 03
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 04
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 05
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 06
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 07
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 08
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 09
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0A
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0B
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0C
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0D
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0E
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0F
-rw-r-----.   1 squid squid 5040 Aug 23 07:52 swap.state
```

## 11.3 清除cache缓存目录

Squid代理服务器的cache缓存目录会自动增大，当用户要求连接时，squid代理服务器就会自动到网络上读取所需数据，连接的网页越多，cache缓存目录就会越大，不过目录的大小是有限制的，所以也需要将不必要的数据删除，以下介绍该如何删除cache缓存目录中的数据。

### 检查cache大小

默认cache缓存目录路径为/var/spool/squid，swap.state文件会随着代理时间渐渐变大，所以有必要清除cache，以免影响服务效率。

```
[root@localhost /]# cd /var/spool/squid    //进入 squid 默认缓存目录
[root@localhost squid]# ll
total 72
```

```
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 00
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 01
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 02
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 03
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 04
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 05
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 06
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 07
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 08
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 09
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0A
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0B
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0C
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0D
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0E
drwxr-x---. 258 squid squid 4096 Aug 23 07:51 0F
-rw-r-----.   1 squid squid 5760 Aug 23 07:57 swap.state
                                              //cache 文件会越来越大
```

## 清除cache缓存目录

进入cache缓存目录，先关闭squid代理服务，然后删除swap.state文件，再次检查swap.state文件，确认swap.state删除后，重新启动squid代理服务。

```
[root@localhost /]# cd /var/spool/squid       //进入默认缓存目录
[root@localhost squid]# service squid stop    //关闭 squid 代理服务
Stopping squid: ................                           [  OK  ]
[root@localhost squid]# rm -rf  /var/spool/squid/swap.state   //删除缓存文件
[root@localhost squid]# ll
total 64
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 00
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 01
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 02
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 03
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 04
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 05
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 06
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 07
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 08
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 09
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0A
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0B
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0C
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0D
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0E
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0F
-rw-r-----.   1 squid squid    0 Aug 23 09:51 swap.state.last-clean
[root@localhost squid]# service squid start   //启动 squid 服务
Starting squid: .                                          [  OK  ]
```

### 检查是否已正确清除cache

删除swap.state后，启动服务开放给用户继续使用后，检查cache缓存目录内是否有新建立的swap.state，新的swap.state文件容量极小，表示以上操作都成功，建议将删除swap.state加入计划任务中，这样可以让squid代理服务器运行流畅。

```
[root@localhost squid]# ll            //查看缓存目录
total 68
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 00
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 01
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 02
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 03
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 04
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 05
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 06
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 07
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 08
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 09
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0A
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0B
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0C
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0D
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0E
drwxr-x---. 258 squid squid 4096 Aug 23 09:32 0F
-rw-r-----.   1 squid squid   72 Aug 23 09:54 swap.state
                                //缓存目录文件内容清除成功
```

## 11.4 配置Squid连接限制

Squid代理服务器可有效管理连接限制，可以让squid代理服务器的效率及带宽达到有效的利用，如果不做任何配置，任何人都可以使用Proxy服务器，会对squid代理服务器的效率及带宽有带有大负担，尤其是带宽，如果使用不当，有可能会拖垮网络环境。

### 限制指定网段（192.168.233.10~192.168.233.20）无法连接

squid代理服务器可限制某一网段不可以使用Proxy服务器，其他网段可以使用。编辑squid配置文件，使用ACL语法配置所要限制的网段IP地址，然后限制此段ACL不可以使用Proxy服务器。

```
[root@localhost /]# vi /etc/squid/squid.conf
…中间省略…
acl clientdeny src 192.168.233.10-192.168.233.20/32 //限制网段
http_access deny clientdeny              //限制读取网络
```

> **说明**
> 可以自行定义clientdeny连接名称，不过要上下两行一致，否则不会生效。

修改squid代理服务器配置文件后，必须重新启动服务，否则配置不会生效。

```
[root@localhost /]# service squid restart
Stopping squid: ................                        [  OK  ]
Starting squid: .                                       [  OK  ]
```

配置限制网段后，下面来测试配置结果，限制网段的PC使用Proxy服务器时都会被禁止连接，如下图所示。

**ERROR**

**The requested URL could not be retrieved**

当尝试取回该 URL 时遇到下面的错误：http://www.baidu.com/

**访问被拒绝。**

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

缓存服务器的管理员 root.

已由 CentOS-6 (squid/3.1.10) 生成 Fri, 31 Aug 2012 23:54:24 GMT

## 限制某IP地址无法连接

squid代理服务器可以限制某一IP地址不可以使用，其他IP地址都可以使用。编辑squid配置文件，使用ACL语法配置所要限制的IP地址。

```
[root@localhost /]# vi /etc/squid/squid.conf
acl clientdeny src 192.168.233.100/32          //限制此 IP 地址不可以连接
http_access deny clientdeny
```

> **说明**
> 可以自行定义clientdeny连接名称，不过要上下两行一致，否则不会生效。

修改squid代理服务器配置文件后，必须重新启动服务，否则配置不会生效。

```
[root@localhost /]# service squid restart
Stopping squid: ................                        [  OK  ]
Starting squid: .                                       [  OK  ]
```

限制IP地址后，来测试配置结果，所限制的IP地址使用Proxy服务器时都会被禁止连接，所呈现的信息与限制网段的信息相同。

## 限制读取指定的网站

squid代理服务器限制用户不可以连接到特定网站，其他网站都可以正常连接。编辑squid

配置文件，使用ACL语法配置所要限制的网站。例如，要限制yahoo所有的网址，则输入内容是.yahoo.com.cn，如果只是yahoo首页，则输入内容为www. yahoo.com.cn。

```
[root@localhost /]# vi /etc/squid/squid.conf
acl domain dstdomain .yahoo.com.cn        //配置限制的域名
http_access deny domain              //禁止连接的网站
```

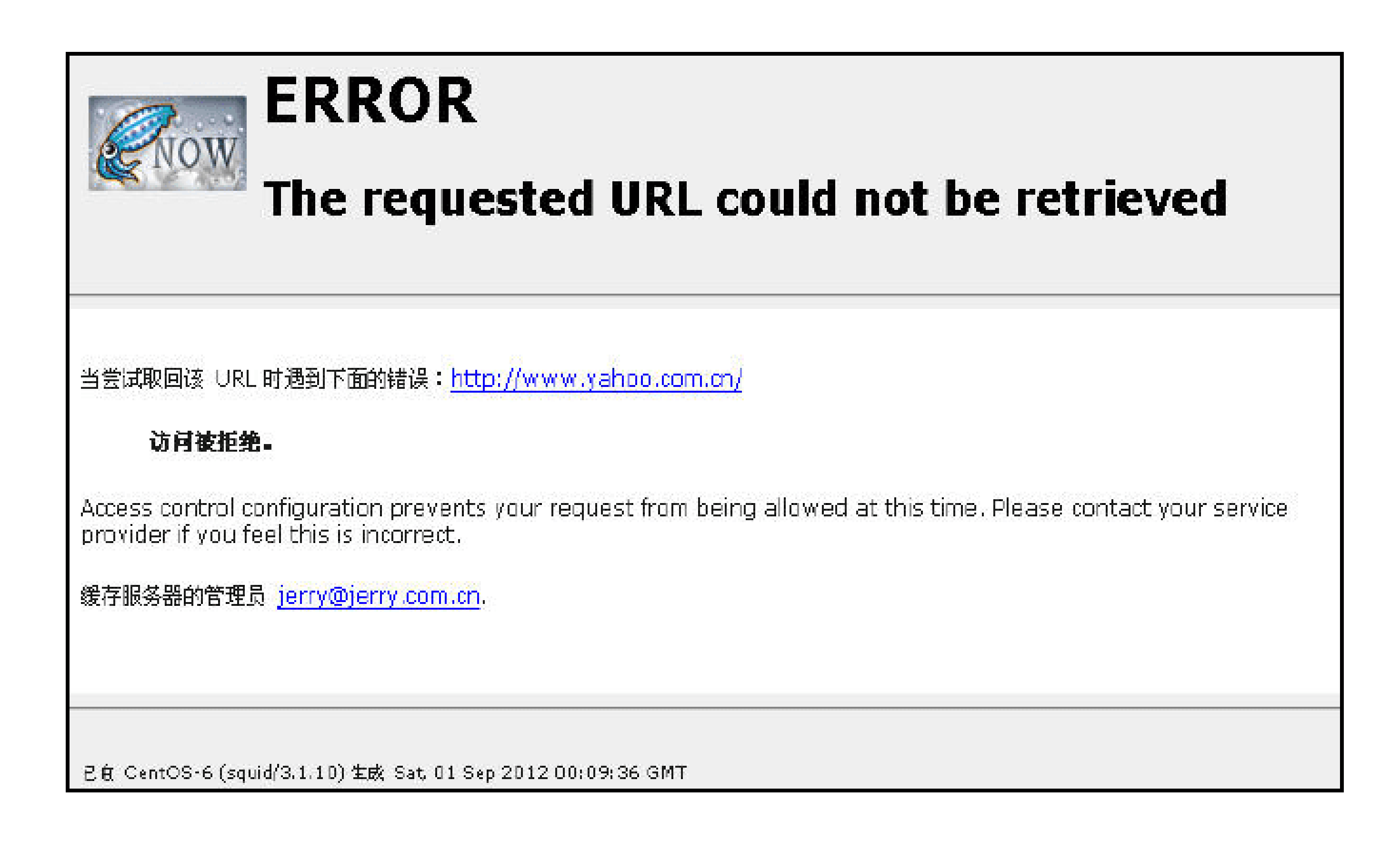
说明

domain连接名称可以自行定义，不过要上下两行一致，否则不会生效。

修改squid代理服务器配置文件后，必须重新启动服务，否则配置不会生效。

```
[root@localhost /]# service squid restart
Stopping squid: ................                          [  OK  ]
Starting squid: .                                         [  OK  ]
```

squid代理服务器服务重新启动后，测试配置结果，yahoo网站确实不可以连接。




## 配置禁止网站清单

Squid代理服务器可以配置拦截网站，不过如果网站太多，一个一个输入后，配置文件会很乱，不好管理，如果可以配置拦截网站清单，配置文件就会比较简洁，以下步骤说明如何配置一份拦截网站的清单。当用户要求连接时，squid代理服务器会对比列表，如果该网站不在清单内，则可以正常浏览，清单内如果有该网址，则不允许连接。

在/etc/squid/目录下建立一份拦截网站清单，文件名为urldeny.txt，拦截yahoo.com.cn及pchoe.com两个网址。

```
[root@localhost /]# vi /etc/squid/urldeny.txt
.pchome.com
.yahoo.com.cn
```

**说明**

拦截网站清单文件的文件名可以自定义，不过要与ACL内容一致。

编辑squid配置文件，使用ACL语法配置拦截网站列表，先输入拦截网站列表的文件路径，再将之设为拦截连接。

```
[root@localhost /]# vi /etc/squid/squid.conf
acl denyurl url_regex "/etc/squid/urldeny.txt"//配置拦截文件和路径
http_access deny denyurl           //拦截清单内的网址
```

Squid代理服务器配置文件修改后，必须重新启动服务，否则配置不会生效。

```
[root@localhost /]# service squid restart
Stopping squid: ................                    [  OK  ]
Starting squid: .                                   [  OK  ]
```

重新启动服务后，打开浏览器，输入【http://www.yahoo.com.cn】，会显示如下信息，这代表拦截网站清单配置成功。

**ERROR**

**The requested URL could not be retrieved**

当尝试取回该 URL 时遇到下面的错误：http://www.yahoo.com.cn/

**访问被拒绝。**

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

缓存服务器的管理员 root.

已由 CentOS-6 (squid/3.1.10) 生成 Sat, 01 Sep 2012 00:19:21 GMT

## 限制用户连接时间

Squid代理服务器可以限制用户在规定的时间范围内连接不到特定网址，其他时间皆可以正常连接。编辑squid配置文件，使用ACL语法配置所要限制的时间。例如，限制每个星期天的11:00~12:00不可以连接。

```
[root@localhost /]# vi /etc/squid/squid.conf
acl timedeny time S 11:00-12:00                          //限制连接时间
http_access deny timedeny
```

说明

timedeny连接名称可以自行定义，不过要上下两行一致，否则不会生效。

星期及英文代码如下表所示。

| 星期 | 一 | 二 | 三 | 四 | 五 | 六 | 天 |
|---|---|---|---|---|---|---|---|
| 代码 | M | T | W | H | F | A | S |

squid代理服务器配置文件修改后，必须重新启动服务，否则配置不会生效。只要用户在该时段使用Proxy服务器就会无法连接。

```
[root@localhost /]# service squid restart
Stopping squid: ................                        [  OK  ]
Starting squid: .                                       [  OK  ]
```

## 11.5 使用ncsa_auth 认证

Proxy服务器目前是被广泛使用的代理服务器，网络上有很多的Proxy List网站，专门收集对外服务的Proxy服务器，每天都会更新，不过这些网站都是由一些软件去扫描3128或80 Port，所以很多未经配置的Proxy服务器常常都是榜上有名，一旦被公开使用，不仅会拖慢网络速度，也很容易被当成跳板使用，建议在Proxy服务器加上一层账户认证和密码保护，即使用Proxy服务器时必须输入账号和密码才可以使用，如果账号和密码未通过的话，就无法使用Proxy服务器，这样就可以减少Proxy服务器被使用在不当的地方。认证账号密码的方式有两种，一种是对LDAP认证，一种是使用htpasswd建立认证账号和密码，这里使用htpasswd建立认证账号和密码方式。

### 建立Squid认证账号和密码

使用htpasswd建立squid认证账号和密码，并配置为所有人都可读。

```
[root@localhost /]# htpasswd -c /etc/squid/passwd jerry
                         //建立 Squid 认证账号和密码
New password:
Re-type new password:
Adding password for user jerry
[root@localhost /]# chmod o+r /etc/squid/passwd   //配置为所有人都可读
```

### 检查 nsca_auth认证服务

检查nsca_auth目录位置，确定nsca_auth目录为/usr/lib64/squid/ncsa_auth。

```
[root@localhost /]# rpm -ql squid | grep ncsa_auth //检查 nsca_auth 目录位置
/usr/lib64/squid/ncsa_auth
/usr/share/man/man8/ncsa_auth.8.gz
```

## 配置Squid认证使用nsca_auth

CentOS 6.x之前的版本，配置文件内容很多，但是之后的版本内容减少许多，都必须要自行配置输入，配置使用nsca_auth认证方式。位置是很重要的，有几点要注意，第一，auth_parm一定要在acl前面，否则会出现Can't use proxy auth because no authentication schemes are fully configured错误；第二，要将auth_parm放在最前面，否则不会出现认证窗口。

```
[root@localhost /]# vi /etc/squid/squid.conf
#
auth_param basic program /usr/lib64/squid/ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Welcome proxy-squid web server
// 认证方式及账号和密码位置
// 5 个程序来验证需求
// 登入时欢迎词
# Recommended minimum configuration:
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl localhost src ::1/128
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32
acl to_localhost dst ::1/128
acl squid_user proxy_auth REQUIRED                              //验证的 ACL
http_access allow squid_user
```

| | |
|---|---|
| /usr/lib64/squid/ncsa_auth | nsca_auth 目录位置 |
| /etc/squid/passwd | squid 认证密码位置 |

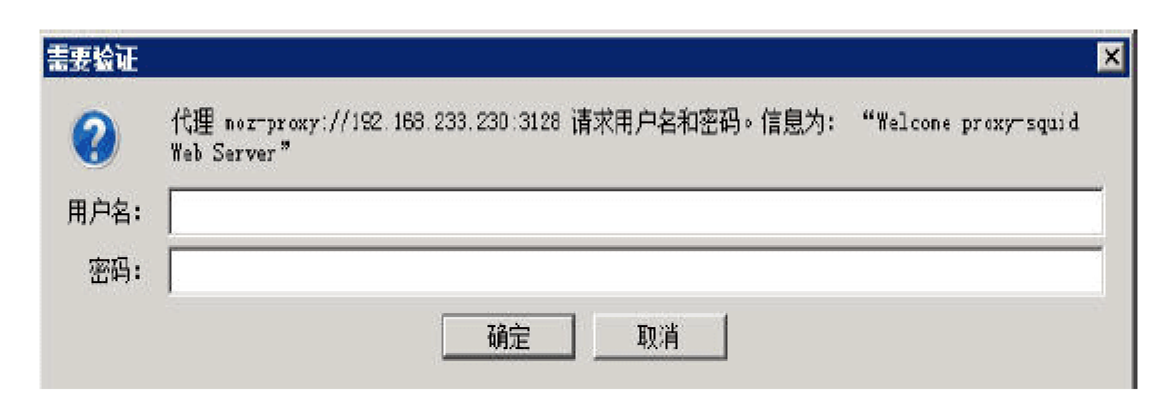
> **说明**
> 记得要启动Apache服务，如果没有安装Apache，请先安装。

Squid代理服务器配置完成后，必须重新启动服务，配置才会生效。

```
[root@localhost /]# service squid restart
Stopping squid: ................                        [  OK  ]
Starting squid: .                                       [  OK  ]
```

## 测试Squid认证服务

如果已预先配置好使用Proxy服务器，打开浏览器会先跳出一个询问Squid账号和密码的对话框。



输入squid代理服务器的认证账号和密码，squid代理服务器认证成功后，即可以正常使用Proxy服务器浏览网页，如下图所示。




如果认证账号和密码输入错误或没有输入账号和密码，则无法浏览网页，如下图所示，请重新输入或检查账号和密码是否有误。




## 11.6 SARG监控squid代理服务器

SARG官方网站：http://sarg.sourceforge.net/。

squid代理服务器的缺点就是记录文件过于复杂，一般来说要完全阅读CentOS操作系统的记录文件是非常困难的，所以必须依赖其他工具来整理，Squid Analysis Report Generator（SARG）产生的报表可以让我们轻松地掌握squid代理服务器的使用记录，以便了解Proxy服务器的运行。

在安装SARG软件前，必须要安装Apache网页服务器，因为SARG以网页方式呈现，所以必须要安装Apache并启动。

### 下载SARG软件

可以从官方网站下载SARG软件，或者可以使用其他网站包装好的RPM安装，在此使用

RPM安装，目前没有看到el6的软件，不过el5的软件一样可以使用。

```
[root@localhost ]# wget http://pkgs.repoforge.org/sarg/sarg-2.3-1.el5.rf.x86_64.rpm
…中间省略…
Saving to: "sarg-2.3-1.el5.rf.x86_64.rpm"
100%[=================================================>] 323,184      142K/s   in 2.2s
2012-08-30 04:27:27 (142 KB/s) - "sarg-2.3-1.el5.rf.x86_64.rpm" saved [323184/323184]
```

说明

SARG文件的来源：http://dag.wieers.com/rpm/packages/sarg/。

安装SARG软件时发生错误，错误信息显示SARG必须安装GD软件。

```
[root@localhost ~]# rpm -ivh sarg-2.3-1.el5.rf.x86_64.rpm
warning: sarg-2.3-1.el5.rf.x86_64.rpm: Header V3 DSA/SHA1 Signature, key ID 6b8d79e6:
NOKEY
error: Failed dependencies:
        gd >= 1.8 is needed by sarg-2.3-1.el5.rf.x86_64
        libgd.so.2() (64bit) is needed by sarg-2.3-1.el5.rf.x86_64
```

由于缺少GD软件，所以由yum在线更新方式进行安装。

```
[root@localhost /]# yum install -y gd    //安装 GD 软件
Dependencies Resolved
======================================================================
 Package         Arch          Version                  Repository      Size
======================================================================
Installing:
 gd            x86_64        2.0.35-10.el6            base          142 k
Transaction Summary
======================================================================
Install        1 Package(s)
Upgrade        0 Package(s)
Total download size: 142 k
```

GD软件安装完毕后，再次安装SARG的rpm文件，则可以安装成功。

```
[root@localhost ~]# rpm -ivh sarg-2.3-1.el5.rf.x86_64.rpm
warning: sarg-2.3-1.el5.rf.x86_64.rpm: Header V3 DSA/SHA1 Signature, key ID 6b8d79e6:
NOKEY
Preparing...                ########################################### [100%]
   1:sarg                   ########################################### [100%]
```

## 编辑/etc/httpd/conf.d下的SARG配置文件

编辑sarg配置文件，默认只允许本机IP地址浏览。如果要让所有人都可以浏览，必须使所有网段允许连接。

```
[root@localhost html]# vi /etc/httpd/conf.d/sarg.conf
Alias /sarg /var/www/sarg
<Directory /var/www/sarg>
        DirectoryIndex index.html
        Order deny,allow
#       Deny from all       //取消限制所有网段不可以连接
        Allow from all
#       Allow from 127.0.0.1      //停用只允许本机 IPv4 连接
#       Allow from ::1      //停用只允许本机 IPv6 连接
        # Allow from your-workstation.com
</Directory>
```

说明

如果没有修改上述配置会出现错误信息，显示没有权限，如下图所示。

**Forbidden**

You don't have permission to access /sarg/ on this server.

*Apache/2.2.15 (CentOS) Server at 192.168.233.230 Port 80*

## 配置SARG配置文件

SARG配置文件内有很多配置，不过刚安装好SARG后，不一定要马上配置，可以将下列几个配置值作为参考。

```
[root@localhost ~]# vi /etc/sarg/sarg.conf
# sarg.conf
#
# TAG:  language
…中间省略…
#language English
              //默认为英文，如果有中文语言包可以切换语言，如果要使用其他语言，要将#移除
…中间省略…
# TAG:  access_log file
#       Where is the access.log file
#       sarg -l file
#
#access_log /usr/local/squid/var/logs/access.log
access_log /var/log/squid/access.log       //分析日志文件位置
…中间省略…
# TAG:  title
#       Especify the title for html page.
#
#title "Squid User Access Reports"         //网站标题名称
…中间省略…
# TAG:  temporary_dir
#       Temporary directory name for work files
#       sarg -w dir
#
```

```
#temporary_dir /tmp                //分析数据存储位置
…中间省略…
# TAG:  output_dir
#       The reports will be saved in that directory
#       sarg -o dir
#
#output_dir /var/www/html/squid-reports
output_dir /var/www/sarg/ONE-SHOT          //分析数据生成位置
…中间省略…
# TAG:  output_email
#       Email address to send the reports. If you use this tag, no html reports will be
generated.
#       sarg -e email
#
#output_email none
…中间省略…
# TAG: charset name
#      ISO 8859 is a full series of 10 standardized multilingual single-byte coded (8bit)
#       graphic character sets for writing in alphabetic languages
#       You can use the following charsets:
#                Latin1          - West European
#                Latin2          - East European
#                Latin3          - South European
#                Latin4          - North European
#                Cyrillic
#                Arabic
#                Greek
#                Hebrew
#                Latin5          - Turkish
#                Latin6
#                Windows-1251
#                Koi8-r
#
#charset Latin1                //网页编码
```

## 重新启动Apache服务

编辑SARG配置文件，根据需求修改配置，修改所有配置后，必须重新启动Apache服务器，否则配置无法生效。

```
[root@localhost ~]# service httpd restart        //重新启动 Apache
Stopping httpd:                                          [  OK  ]
Starting httpd:                                          [  OK  ]
```

## 生成每日、周、月报表

SARG可以根据日、周、月报表收集squid代理服务器的数据。建议自行加入计划任务以便每天生成。

```
[root@localhost ~]# sarg -o /var/www/sarg/ONE-SHOT  //一次报表
SARG: Records in file: 1357, reading: 100.00%
[root@localhost ~]# sarg -o /var/www/sarg/daily     //日报表
```

```
SARG: Records in file: 1357, reading: 100.00%
[root@localhost ~]# sarg -o /var/www/sarg/weekly    //周报表
SARG: Records in file: 1357, reading: 100.00%
[root@localhost ~]# sarg -o /var/www/sarg/monthly   //月报表
SARG: Records in file: 1357, reading: 100.00%
```

## SARG报表

打开浏览器，输入【http://IP/sarg】，就可以开启SARG首页，SARG报表分为一次、日、周、月报表。

**Squid User's Access Report**

| DIRECTORY | DESCRIPTION |
|---|---|
| ONE-SHOT | One shot reports |
| daily | Daily reports |
| weekly | Weekly reports |
| monthly | Monthly reports |

SARG会依每个时间平均产生流量报表，单击进入可以看到更多信息。

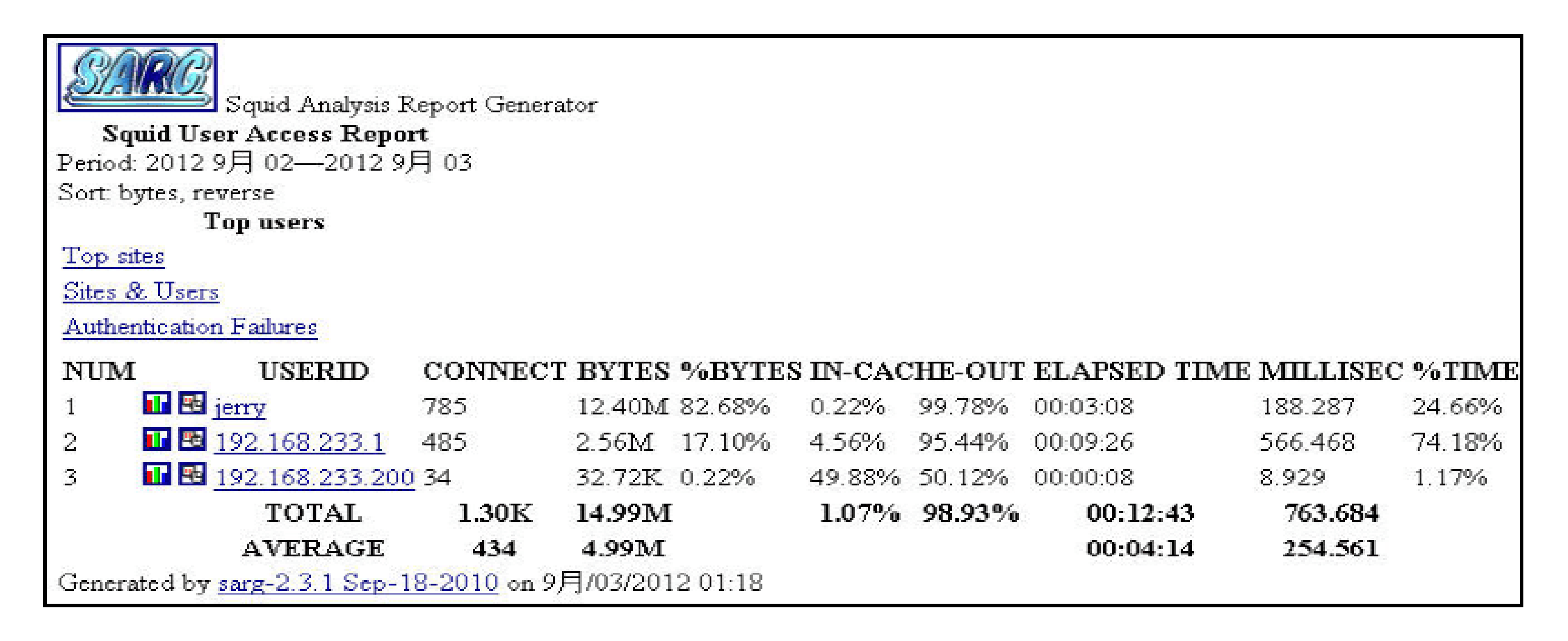


Squid Analysis Report Generator
Squid User Access Report

| FILE/PERIOD | CREATION DATE | USERS | BYTES | AVERAGE |
|---|---|---|---|---|
| 2012Sep02-2012Sep03 | 2012年09月03日 星期一 00时58分19秒 | 2 | 2.34M | 1.17M |
| 2012Sep02-2012Sep03.7 | 2012年09月03日 星期一 00时57分50秒 | 2 | 2.34M | 1.17M |

Generated by sarg-2.3.1 Sep-18-2010 on 9月/03/2012 00:58

SARG会对每个IP地址做流量的统计表。



Squid Analysis Report Generator
Squid User Access Report
Period: 2012 9月 02—2012 9月 03
Sort: bytes, reverse
Top users
Top sites
Sites & Users
Authentication Failures

| NUM | USERID | CONNECT | BYTES | %BYTES | IN-CACHE-OUT | | ELAPSED TIME | MILLISEC | %TIME |
|---|---|---|---|---|---|---|---|---|---|
| 1 | jerry | 785 | 12.40M | 82.68% | 0.22% | 99.78% | 00:03:08 | 188.287 | 24.66% |
| 2 | 192.168.233.1 | 485 | 2.56M | 17.10% | 4.56% | 95.44% | 00:09:26 | 566.468 | 74.18% |
| 3 | 192.168.233.200 | 34 | 32.72K | 0.22% | 49.88% | 50.12% | 00:00:08 | 8.929 | 1.17% |
| | TOTAL | 1.30K | 14.99M | | 1.07% | 98.93% | 00:12:43 | 763.684 | |
| | AVERAGE | 434 | 4.99M | | | | 00:04:14 | 254.561 | |

Generated by sarg-2.3.1 Sep-18-2010 on 9月/03/2012 01:18

单击该IP地址，可以查看所有浏览过网站的统计资料。

SARG Squid Analysis Report Generator

**Squid User Access Report**

Period: 2012 9月 02—2012 9月 03

User: 192.168.233.1

Sort: bytes, reverse

**User report**

| ACCESSED SITE | CONNECT | BYTES | %BYTES | IN-CACHE-OUT | | ELAPSED TIME | MILLISEC | %TIME |
|---|---|---|---|---|---|---|---|---|
| safebrowsing-cache.google.com | 153 | 711.11K | 27.73% | 0.00% | 100.00% | 00:00:17 | 17.495 | 3.09% |
| i.firefoxchina.cn | 16 | 307.06K | 11.97% | 0.00% | 100.00% | 00:00:01 | 1.234 | 0.22% |
| 192.168.233.230 | 122 | 286.15K | 11.16% | 2.41% | 97.59% | 00:00:03 | 3.172 | 0.56% |
| himg2.huanqiu.com | 32 | 268.71K | 10.48% | 2.60% | 97.40% | 00:08:28 | 508.945 | 89.85% |
| www.iegallery.com | 2 | 139.29K | 5.43% | 0.00% | 100.00% | 00:00:01 | 1.982 | 0.35% |
| img.taobaocdn.com | 5 | 105.26K | 4.10% | 0.00% | 100.00% | 00:00:00 | 976 | 0.17% |
| s1.bdstatic.com | 8 | 95.56K | 3.73% | 100.00% | 0.00% | 00:00:00 | 15 | 0.00% |

# 11.7 Dansguardian过滤不当网站

Dansguardian官方网站：http://dansguardian.org。

Dansguardian 是一套免费的Proxy filter，可以帮助我们限制Client 端访问不应该访问的网页，它具有强大的功能。Dansguardian 所具备的特征有：执行速度很快、要求的计算机资源不大，可以过滤指定的URL 或IP，可以指定哪些文件不可以下载，如mp3、vbs等。Content filtering 是指过滤网页的内容。

## 下载Dansguardian软件

Dansguardian软件可以从官方网站下载，或者可以使用其他网站包装好的RPM安装，在此使用RPM安装。

```
[root@localhost ~]# wget
http://pkgs.repoforge.org/dansguardian/dansguardian-2.10.1.1-1.el6.rf.x86_64.rpm
Saving to: "dansguardian-2.10.1.1-1.el6.rf.x86_64.rpm"
100%[=====================================================>] 463,096     57.5K/s   in 8.1s
2012-08-30 05:47:43 (56.0 KB/s) - "dansguardian-2.10.1.1-1.el6.rf.x86_64.rpm" saved
[463096/463096]
```

## 安装Dansguardian 软件

下载好 Dansguardian 的 rpm 文件后，即可安装 Dansguardian。

```
[root@localhost ~]# rpm -ivh dansguardian-2.10.1.1-1.el6.rf.x86_64.rpm
warning: dansguardian-2.10.1.1-1.el6.rf.x86_64.rpm: Header V3 DSA/SHA1 Signature, key ID
6b8d79e6: NOKEY
Preparing...                ########################################### [100%]
   1:dansguardian           ########################################### [100%]
```

## 修改配置文件

安装Dansguardian后，必须做一些与Proxy服务器之间的配置，否则无法使用。编辑

Dansguardian配置文件，配置Dansguardian语言，默认为ukenglish，将之改成简体中文。

```
[root@localhost ~]# vi /etc/dansguardian/dansguardian.conf
# Language dir where languages are stored for internationalisation.
# The HTML template within this dir is only used when reportinglevel
# is set to 3. When used, DansGuardian will display the HTML file instead of
# using the perl cgi script.  This option is faster, cleaner
# and easier to customise the access denied page.
# The language file is used no matter what setting however.
#
languagedir = '/usr/share/dansguardian/languages'           //语言文件目录
# language to use from languagedir.
language = 'chinesegb2312'//默认为 ukenglish 英文，修改为简体中文 chinesegb2312
```

如果不确定是否有需要的语言包，查看languagedir语言包目录/etc/dansguardian/languages，查找需要的语言包。

```
[root@localhost ~]# ll /usr/share/dansguardian/languages
total 108
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 arspanish
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 bulgarian
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 chinesebig5
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 chinesegb2312
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 czech
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 danish
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 dutch
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 french
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 german
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 hebrew
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 hungarian
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 indonesian
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 italian
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 japanese
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 lithuanian
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 malay
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 mxspanish
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 polish
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 portuguese
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 ptbrazilian
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 russian-1251
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 russian-koi8-r
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 slovak
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 spanish
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 swedish
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 turkish
drwxr-xr-x. 2 dansguardian dansguardian 4096 Aug 30 05:49 ukenglish
```

编辑Dansguardian配置文件，filterport配置Dansguardian使用的端口默认为8080，如果无冲突，建议不用修改。Dansguardian使用的Proxy服务器的IP地址，默认为127.0.0.1，如果

Dansguardian与Proxy Server 是在同一主机上，则无需修改，如果是在另一台主机上则必须配置该主机IP。配置Dansguardian使用的Proxy主机Port，默认为3128，若Dansguardian与Proxy Server 是在同一主机上，则无需修改，如果是在另一台主机上则必须配置该主机Proxy使用的Proxy Port。如果使用简体中文，必须将forcequicksearch设为on，默认为off。

```
[root@localhost ~]# vi /etc/dansguardian/dansguardian.conf
# Network Settings
#
# the IP that DansGuardian listens on.  If left blank DansGuardian will
# listen on all IPs.  That would include all NICs, loopback, modem, etc.
# Normally you would have your firewall protecting this, but if you want
# you can limit it to a certain IP. To bind to multiple interfaces,
# specify each IP on an individual filterip line.
filterip =

# the port that DansGuardian listens to.
filterport = 8080                                //默认 Dansguardian 端口

# the ip of the proxy (default is the loopback - i.e. this server)
proxyip = 127.0.0.1
  //Proxy 服务器与 Dansguardian 在同一主机，则无需修改，否则必须配置为该 Proxy 服务器

# the port DansGuardian connects to proxy on
proxyport = 3128
               //该 Proxy 服务器端口为 3128，则无需修改，否则需修改为相对的端口

…中间省略…
# Force Quick Search rather than DFA search algorithm
# The current DFA implementation is not totally 16-bit character compatible
# but is used by default as it handles large phrase lists much faster.
# If you wish to use a large number of 16-bit character phrases then
# enable this option.
# off (default) | on (Big5 compatible)
forcequicksearch = on                                //默认为 off，必须设为 on
```

## 配置防火墙

Dansguardian需在防火墙中开启8080端口，这样才可以对外连接，否则无法使用。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 3128 -j ACCEPT
```

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
                                                    // Dansguardian 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完毕后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                          [  OK  ]
iptables: Setting chains to policy ACCEPT: filter           [  OK  ]
iptables: Unloading modules:                                [  OK  ]
iptables: Applying firewall rules:                          [  OK  ]
```

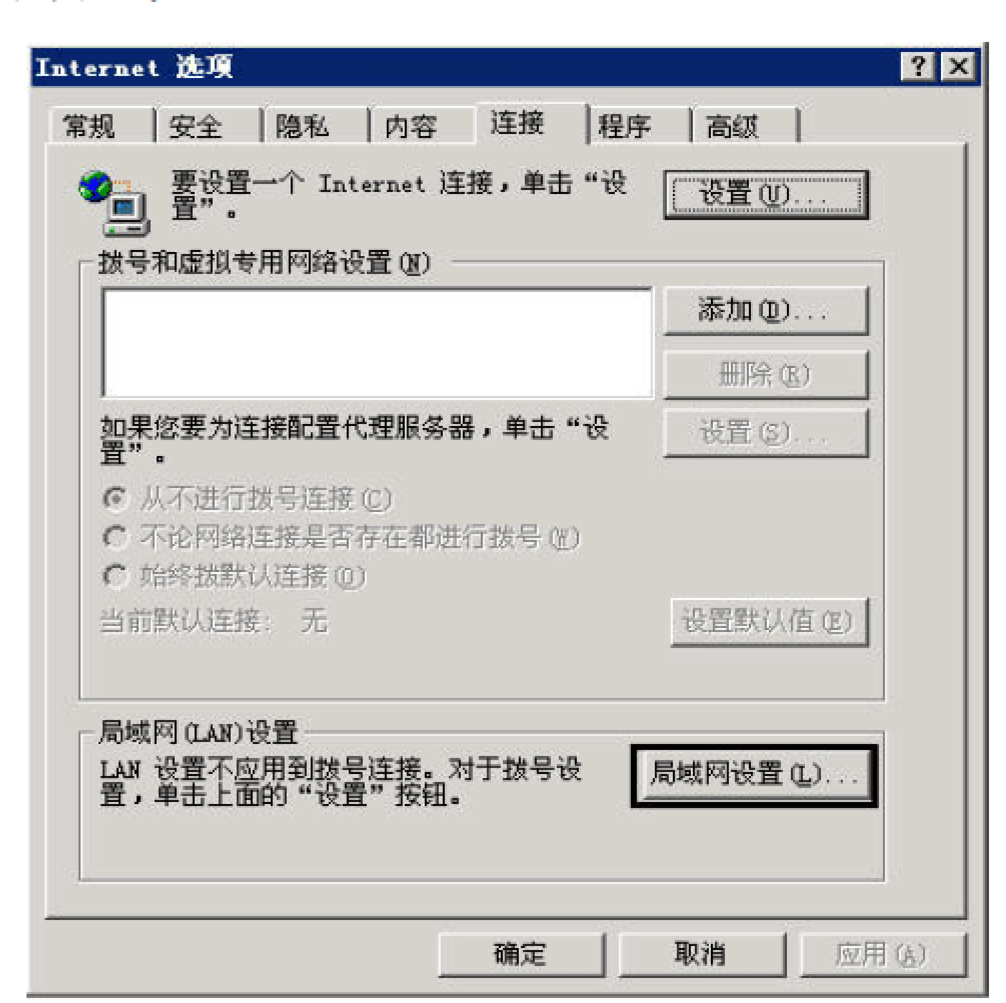
## 启动Dansguardian服务

一切配置完成后，就可以启动Dansguardian了，请将Dansguardian配置为默认启动，输入【chkconfig dansguardian on】，以免重新启动后，启动squid时忘记启动Dansguardian。

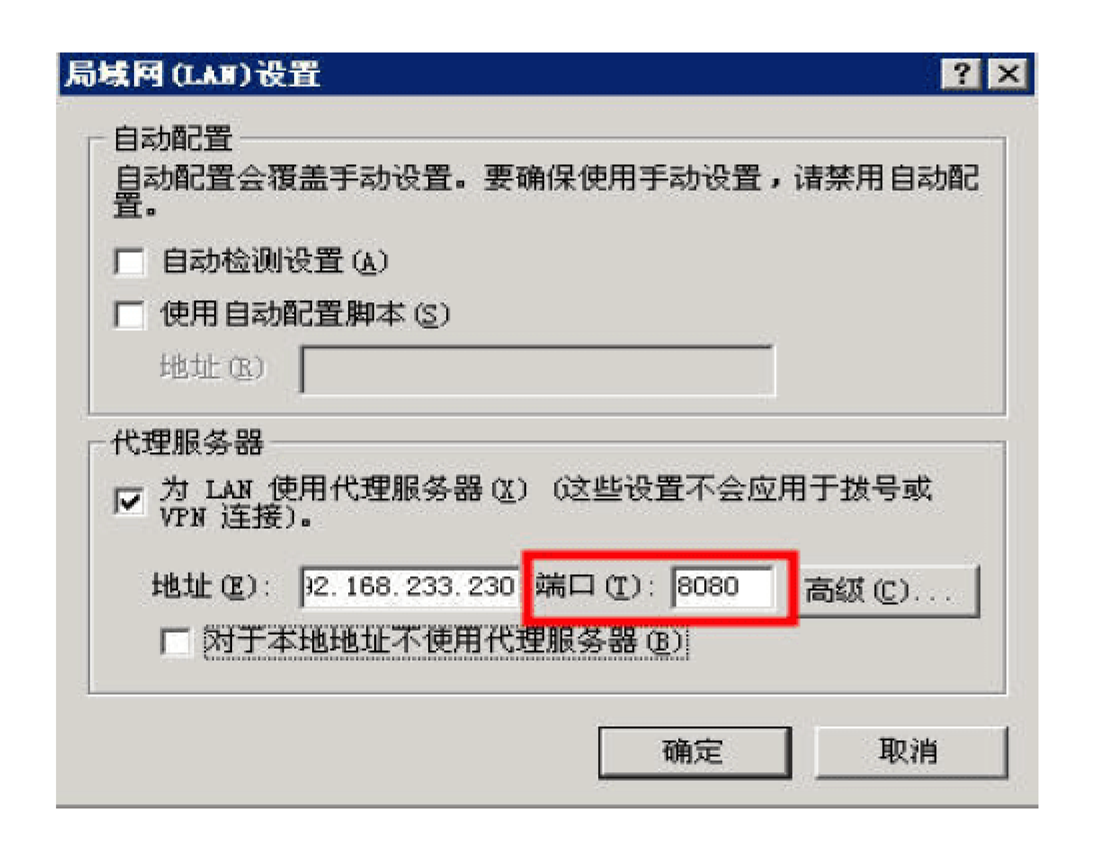
```
[root@localhost ~]# service dansguardian start
Starting Web Content Filter (dansguardian):                  [  OK  ]
```

## 配置客户端

Dansguardian配置完成后，客户端原本使用的是squid代理服务器默认的端口3128，但要使用Dansguardian，就要将配置都指向Dansguardian，打开浏览器，选择【工具】→【Internet选项】→【连接】，单击【局域网设置】。




在【代理服务器】选项中，勾选【为LAN使用代理服务器（这些设置不会应用于拨号或VPN连接）】，将地址配置为Proxy Server的IP地址，将端口配置为Dansguardian的filterport即8080，配置完成后，按【确定】。

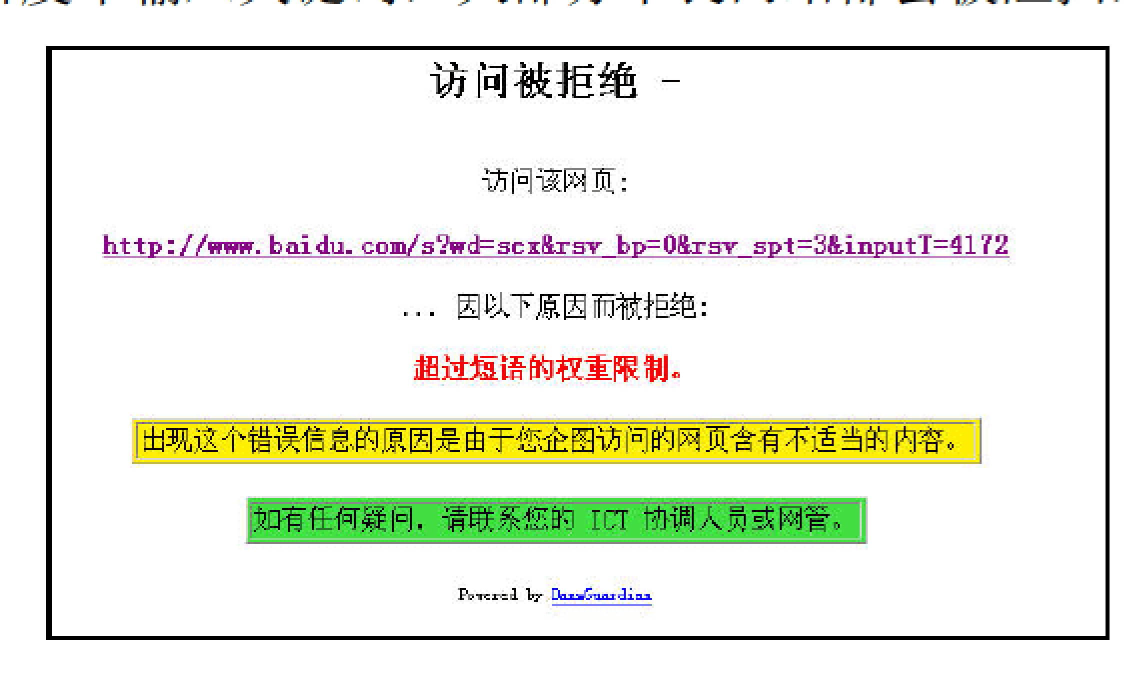



说明

如果用户继续使用端口3128的话，Dansguardian就无法阻挡。

## 测试Dansguardian是否阻挡不良网站

打开浏览器，在百度中输入关键词，大部分不良网站都会被阻挡，如下图所示。




查看Dansguardian纪录文件，可以看到非法字符，说明Dansguardian阻挡成功。

```
[root@localhost lists]# tail -f /var/log/dansguardian/access.log
2012.8.30 7:10:30 - 192.168.233.100 http://www.baidu.com/tbr?
features=Rank:SW&sourceid=navclient-ff&client=navclient-auto-ff&sw=
ui,co,dm&googleip=O;74.125.31.103;177&iqrn=vKv&querytime=Xt&orig=
02dr4&swwk=409&ch=87b5deffa&q=info:http%3A%2F%2Fwww.baidu.com
%2Fsearch%3Fhl%3D%26q%3D%25E6%2584%259B%25E6%2584%259B%26
sourceid%3Dnavclient-ff%26rlz%3D1B3GGLL_zh-TWTW409TW409%26ie%
3DUTF-8  GET 138 0  1 200 text/html   -
2012.8.30 7:10:33 - 192.168.233.100 http://www.baidu.com/favicon.ico
  GET 83 0  1 404 text/html   -
2012.8.30 7:10:41 - 192.168.233.100 http://www.bandu.com/gen_204?atyp=
i&ct=&cad=&ved=0CBgQ_gU&ei=E6xbTs2QJczmmAXlmpSrDA&zx=
1314630689644  GET 0 0  1 204 text/html   -
2012.8.30 7:10:46 - 192.168.233.100 http://www.bandu.com/url?sa=t&source=
web&cd=4&ved=0CDgQFjAD&url=http%3A%2F%2Fwww.wo-xxxx.com.cn%
2Farticle.aspx%3Fcid%3D67%26id%3D2291&ei=E6xbTs2QJczmmAXlmpSrDA
&usg=AFQjCNE7MRfirvsesjTmzmD-EYG636M-OQ&sig2=2OVbZ4qnHHrv
```

```
WtLT6SrHAw  GET 253 0  1 302 -   -
2012.8.30 7:10:46 - 192.168.233.100 http:// www.wo-xxx.com.cn/article.aspx?cid=
67&id=2291 *DENIED* ▒[▒v▒▒▒y▒r▒y▒▒▒▒50 : 105 (▒▒+女+性感+美) GET 46077 105 Pornography
(Japanese) , Pornography (Chinese) 1 403
 text/html   -
```

## 加入禁止的网址

Bannedsitelist是禁止网站清单，编辑bannedsitelist，加入所要拦截的网站。

```
[root@localhost /]# vi /etc/dansguardian/lists/bannedsitelist
# You will need to edit to add and remove categories you want
Bbs.baidu.com                                                   //阻挡此网站
```

加入拦截网站后，必须重新启动dansguardian，否则配置无法生效。

```
[root@localhost /]# service dansguardian restart
Shutting down Web Content Filter (dansguardian) :           [  OK  ]
Starting Web Content Filter (dansguardian) :                [  OK  ]
```

再次打开浏览器，输入阻挡的网址，就会以禁止网址的方式阻挡该网址。

访问被拒绝 -

访问该网页：

http://bbs.baidu.com

... 因以下原因而被拒绝：

被禁止的网站：bbs.baidu.com

出现这个错误信息的原因是由于您企图访问的网页含有不适当的内容。

如有任何疑问，请联系您的 ICT 协调人员或网管。

Powered by DansGuardian

## 加入禁止的关键词

Bannedphraselist除了有拦截网站的作用，也可以拦截字符，如加入make love关键词。

```
[root@localhost /]# vi /etc/dansguardian/lists/bannedphraselist
…中间省略…
<make love>                                       //阻挡关键词
```

> **说明**
>
> 如果要输入中文词语，必须修改i18n，将LANG="en_US.UTF-8"加上#号并加上LANG="zh_CN.UTF-8"，配置好后重新启动则可以使用，如果使用pietty连接，字符编码要选择zh_CN.UTF-8，并将系统默认去掉。

```
[root@localhost ~]# vi /etc/sysconfig/i18n
#LANG="en_US.UTF-8"
LANG=" zh_CN.UTF-8"
SYSFONT="latarcyrheb-sun16"
```

加入拦截词语后，必须重新启动dansguardian，否则配置无法生效。

```
[root@localhost /]# service dansguardian restart
Shutting down Web Content Filter (dansguardian) :              [  OK  ]
Starting Web Content Filter (dansguardian) :                   [  OK  ]
```

再次打开浏览器，输入拦截的词语，就会出现对禁止词组的阻挡。

访问被拒绝 –
访问该网页：
wd=make+love&rsv_bp=0&rsv_spt=3&inputT=2703
... 因以下原因而被拒绝：
发现被禁止的短语。
出现这个错误信息的原因是由于您企图访问的网页含有不适当的内容。
如有任何疑问，请联系您的 ICT 协调人员或网管。
Powered by DansGuardian

# 禁止下载的文件类型

Bannedextensionlist可以禁止下载的文件类型，默认有一些拦截的文件类型，如果要取消拦截，只要在前面加上#号即可，这里拦截exe文件的下载。

```
[root@localhost /]# vi /etc/dansguardian/lists/bannedextensionlist
#Banned extension list

# File extensions with executable code

# The following file extensions can contain executable code.
# This means they can potentially carry a virus to infect your computer.

.ade  # Microsoft Access project extension
.adp  # Microsoft Access project
.asx  # Windows Media Audio / Video
.bas  # Microsoft Visual Basic class module
.bat  # Batch file
.cab  # Windows setup file
.chm  # Compiled HTML Help file
.cmd  # Microsoft Windows NT Command script
.com  # Microsoft MS-DOS program
.cpl  # Control Panel extension
.crt  # Security certificate
```

```
.dll  # Windows system file
.exe  # Program
.hlp  # Help file
.exe                                          //加入对 exe 文件的阻挡
```

加入拦截文件类型后，必须重新启动dansguardian，否则配置无法生效。

```
[root@localhost /]# service dansguardian restart
Shutting down Web Content Filter (dansguardian) :              [  OK  ]
Starting Web Content Filter (dansguardian) :                   [  OK  ]
```

再次打开浏览器，下载带有exe扩展名的文件，就会出现拦截信息。




# 11.8 实例介绍——限制浏览Facebook的时间

目前很多公司或单位都因为Facebook的小游戏导致网络流量过大或没有工作效率，该如何限制员工只在休息时间才可以浏览Facebook呢？做法如下所示。

## Facebook IP地址查询

使用nslookup方式查询Facebook有哪些IP地址，目前有69.63.189.16、69.63.181.12、69.63.189.11。

```
默认服务器:  dns.hinet.net
Address:  168.95.1.1
> facebook.com
服务器:  dns.hinet.net
Address:  168.95.1.1
未经授权的回答:
facebook.com    internet address = 69.63.189.16
facebook.com    internet address = 69.63.181.12
facebook.com    internet address = 69.63.189.11
facebook.com    nameserver = ns3.facebook.com
facebook.com    nameserver = ns2.facebook.com
```

```
facebook.com     nameserver = ns1.facebook.com
facebook.com     nameserver = ns4.facebook.com
facebook.com     nameserver = ns5.facebook.com
```

> **说明**
>
> Facebook IP地址常常改变，如果未拦截请自行查询。

## 配置限制浏览Facebook的时间

编辑squid配置文件，将阻挡的Facebook IP地址加入，其中ACL部分加入上班时间限制不可以连接Facebook，不过休息时间12:00~13:30例外，可以连接Facebook。

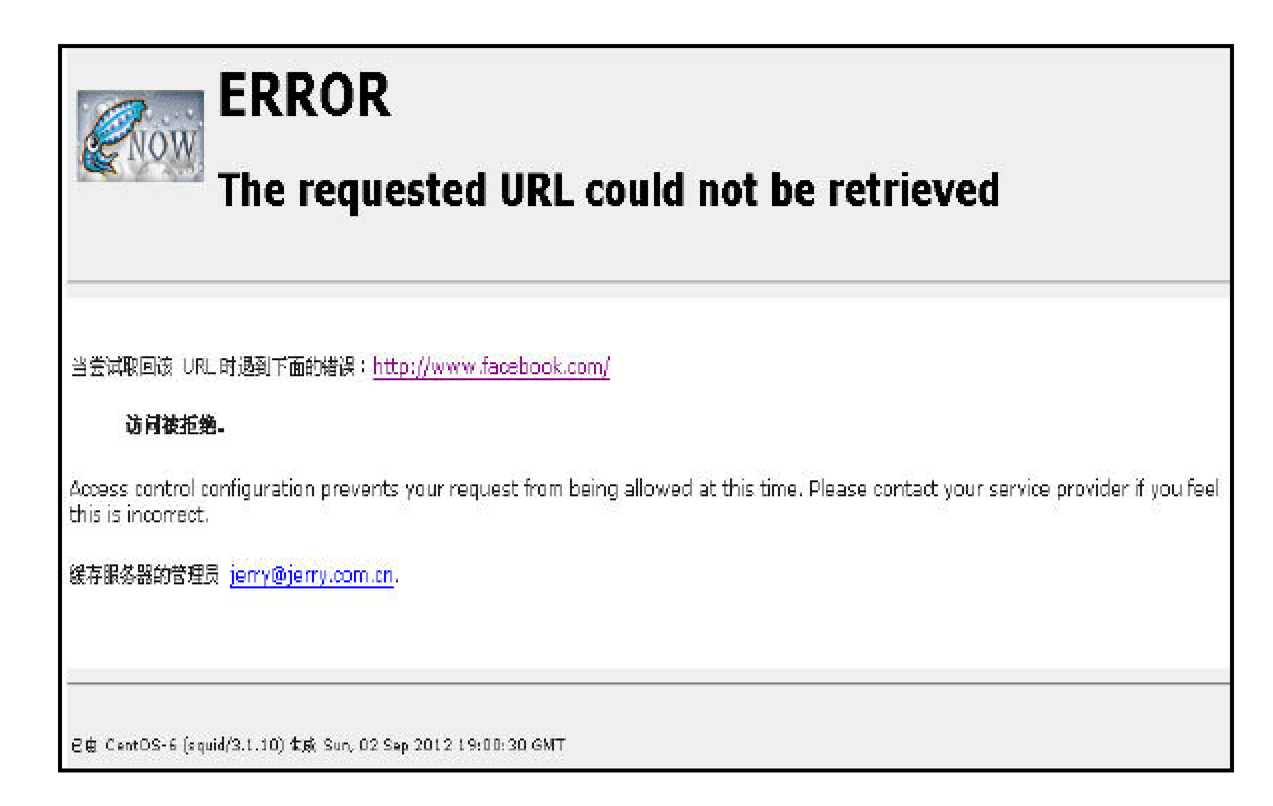
```
[root@localhost ~]# vi /etc/squid/squid.conf
acl worktime time MTWHF 8:30-18:00    //星期一至五 08:30~18:00 为上班时间
acl resttime time 12:00-13:30      //中午休息时间 12:00~13:30
acl deny_domain dstdomain .facebook.com //限制 facebook 网站
acl deny_IP dst 69.63.189.16/32 69.63.181.12/32 69.63.189.11/32
                                //限制 Facebook  IP 地址
http_access allow deny_domain resttime   //开放休息时间浏览 Facebook 网站
http_access allow deny_IP resttime    //开放休息时间可以使用 Facebook IP
http_access deny deny_domain worktime //禁止上班时间浏览 Facebook 网站
http_access deny deny_IP worktime     //禁止上班时间使用 Facebook IP
```

配置完成后，必须重新启动服务，配置值才会生效。

```
[root@localhost ~]# service squid restart
Stopping squid: ...............                           [  OK  ]
Starting squid: .                                         [  OK  ]
```

## Facebook使用时间测试

拦截时间标准以squid服务器为标准。上班时间浏览Facebook网站，会出现下列信息，代表阻挡成功。



休息时间浏览Facebook网站，可以正常打开Facebook网站，如下图所示。



# 第 12 章

# DHCP——动态主机配置服务器

DHCP（Dynamic Host Configuration Protocol）服务器可以让同一网络中的计算机自动获取IP地址。DHCP 服务器让网络中计算机的配置更便利，不用一台一台地去配置计算机的IP地址，对于大型网络环境而言，可以大幅减少管理者的负担。

## 12.1 安装简单的DHCP 服务器

简单的DHCP服务器可以为同网段内的计算机自动分配IP地址、子网掩码、网关、域名、DNS服务器地址等配置信息。

### 检查DHCP服务器软件

配置DHCP服务前，应该先检查是否安装DHCP相关软件。

```
[root@localhost ~]# rpm -qa|grep dhcp
dhcp-4.1.1-12.P1.el6_0.4.x86_64
dhcp-devel-4.1.1-12.P1.el6_0.4.x86_64
```

### 安装DHCP服务器软件

若没有安装DHCP服务器软件，则以yum在线更新的方式进行安装。

```
[root@localhost ~]# yum install -y dhcp dhcp-devel

Dependencies Resolved

======================================================================
 Package        Arch      Version                  Repository       Size
======================================================================
Installing:
```

```
 dhcp           x86_64    12:4.1.1-12.P1.el6_0.4      updates          887 k
 dhcp-devel     x86_64    12:4.1.1-12.P1.el6_0.4      updates          152 k

Transaction Summary
=========================================================================
Install       2 Package(s)
Upgrade       0 Package(s)

Total download size: 1.0 M
Installed size: 2.4 M
```

## DHCP配置文件说明

配置DHCP服务器时需要知道每一个参数的作用，就好比配置网卡参数时要知道每个参数的含义一样，DHCP模板配置文件的位置为/usr/share/doc/dhcp-*/dhcpd.conf.sample。

> 说明
>
> 如果DHCP版本为4.1.1版，DHCP模板目录的位置为/usr/share/doc/dhcp-4.1.1，请根据版本编辑对应的模板配置文件。

| 参数 | 参数说明 |
|---|---|
| option routers | 为 DHCP 客户端设置默认网关 |
| option subnet-mask | 为 DHCP 客户端设置子网掩码 |
| option nis-domain | 为 DHCP 客户端设置 NIS 域名 |
| option domain-name | 为 DHCP 客户端设置网络名称 |
| option domain-name-servers | 为 DHCP 客户端设置 DNS 服务器，若有两台则以 IP1、IP2 地址进行区分 |
| option time-offset | 设置现在的时区和 GMT（格林威治时区）的时差 |
| option ntp-servers | 为 DHCP 客户端设置时间服务器 |
| option netbios-name-servers | 为 DHCP 客户端设置 WINS 服务器 |
| range dynamic-bootp | 设置地址池 |
| default-lease-time | IP 租约时间，默认为 43200 秒（12 小时） |
| max-lease-time | 最大租约时间，默认为 86400 秒（24 小时） |
| hardware ethernet | 指定 DHCP 客户端的 MAC 地址， |
| fixed-address | 指定 DHCP 客户端的 MAC 地址，能获取的 IP 地址 |

## 配置简单的DHCP 服务器

以下介绍如何配置一个简单的DHCP服务器，简单的DHCP Server顾名思义就是说客户端只能获取IP地址等信息，对自动获得的IP地址不进行任何功能限制，比如租约等功能，则所要准备的资料大致如下表所示。

| 参数 | 参数值 |
| --- | --- |
| IP 地址池 | 192.168.233.10~192.168.233.99 |
| 子网掩码（Subnet-mask） | 255.255.255.0 |
| 网关（Default Gateway） | 192.168.233.1 |
| 域名（Domain Name） | jerryit.idv.cn |
| 名称服务器地址（DNS） | 192.168.233.1 及 168.95.1.1 |

所需要的资料准备好后，就可以配置DHCP 服务器，开始编辑DHCP配置文件了。

```
[root@localhost ~]# vi /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
#
# create new
# specify domain name
subnet 192.168.233.0 netmask 255.255.255.0 {
        option routers                  192.168.233.1;
        option subnet-mask              255.255.255.0;
        option domain-name              "jerryit.idv.cn ";
        option domain-name-servers      168.95.1.1,192.168.233.1;
        range 192.168.233.10 192.168.233.99;
}
```

## 启动DHCP 服务器

一切配置完成后，就可以启动DHCP服务器服务了，若是长期提供服务，建议设为系统默认启动，以避免重新启动服务器后忘记启动，导致客户端无法获取IP地址。

```
[root@localhost ~]# service dhcpd start
Starting dhcpd:                                            [  OK  ]
[root@localhost ~]# chkconfig dhcpd on
```

## 客户端测试

使用Windows XP操作系统测试，在命令控制台中输入【ipconfig/renew】，向DHCP Server索取IP地址，下面的信息代表成功索取到IP地址。

```
Windows IP Configuration
        Host Name . . . . . . . . . . . . : user-3d0c157d5a
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
```

```
        DNS Suffix Search List. . . . . . : jerryit.idv.cn

Ethernet adapter 本地连接 2:
        Connection-specific DNS Suffix  . : jerryit.idv.cn
        Description . . . . . . . . . . . : AMD PCNET Family PCI Ethernet Adapter
        Physical Address. . . . . . . . . : 00-0C-29-E6-79-3A
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.233.11
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.233.1
        DHCP Server . . . . . . . . . . . : 192.168.233.195
                                                    //由此 DHCP Server 取得 IP 地址
        DNS Servers . . . . . . . . . . . : 168.95.1.1
                                            192.168.233.1
        Lease Obtained. . . . . . . . . . : 2012 年 8 月 31 日 上午 03:23:14
        Lease Expires . . . . . . . . . . : 2012 年 8 月 31 日 下午 03:23:14
```

确认客户端获取的IP地址、子网掩码、网关及DNS都符合所配置的信息，则代表DHCP服务器配置成功，租约期默认是12小时。

## 12.2 配置DHCP Server租约时间

配置DHCP服务器租约时间是为了有效管理DHCP服务器上的IP地址池，若不配置IP地址的租约时间，则IP地址总有一天会不够用，到时就需要调整IP地址池的范围了，所以客户端获取后很久没有使用的IP地址，租约时间一到，DHCP服务器就会自动收回。

租约时间分为默认租约时间（default-lease-time）与最大租约时间（max-lease-time），这两种租约时间的差别是当默认租约时间大于最大租约时间时，就以最大租约时间为主。一般配置租约时间时只会配置其中一项，通常为默认租约时间。

### 配置DHCP 服务器

以下介绍当同时配置默认租约时间与最大租约时间后，是否以最大租约时间为主。配置时间信息如下表所示。

| 租约时间类别 | 租约时间 |
|---|---|
| 默认租约时间 default-lease-time | 43200 秒（12 小时） |
| 最大租约时间 max-lease-time | 21600 秒（6 小时） |

编辑DHCP服务器配置文件，在原有的DHCP服务器配置文件内增加默认租约时间及最大租约时间，然后保存退出。

```
[root@localhost ~]# vi /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
```

```
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
#
# create new
# specify domain name
subnet 192.168.233.0 netmask 255.255.255.0 {
        option routers                  192.168.233.1;
        option subnet-mask              255.255.255.0;
        option domain-name              "jerryit.idv.cn";
        option domain-name-servers      168.95.1.1,192.168.233.1;
        range 192.168.233.10 192.168.233.99;
        default-lease-time 43200;                          //默认租约时间
        max-lease-time 21600;                              //最大租约时间
}
```

配置完成后，必须重新启动DHCP Server服务，配置才会生效。

```
[root@localhost ~]# service dhcpd restart
Shutting down dhcpd:                                        [  OK  ]
Starting dhcpd:                                             [  OK  ]
```

## 客户端测试

使用Windows XP操作系统测试，在命令控制台中输入【ipconfig/renew】，计算机重新获取IP地址，取得IP地址后，输入【ipconfig/all】检查租约时间，如下所示，起始租约时间到结束租约时间为6小时，因为所配置的默认租约时间大于最大租约时间，所以DHCP服务以最大租约时间为主。

```
Windows IP Configuration
        Host Name . . . . . . . . . . . . : user-3d0c157d5a
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : jerryit.idv.cn

Ethernet adapter 本地连接 2:
        Connection-specific DNS Suffix  . : jerryit.idv.cn
        Description . . . . . . . . . . . : AMD PCNET Family PCI Ethernet Adapter #2
        Physical Address. . . . . . . . . : 00-0C-29-E6-79-44
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.233.50
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.233.1
        DHCP Server . . . . . . . . . . . : 192.168.233.195
        DNS Servers . . . . . . . . . . . : 168.95.1.1
                                            192.168.233.1
        Lease Obtained. . . . . . . . . . : 2012 年 9 月 1 日 上午 12:30:38
```

```
        Lease Expires . . . . . . . . . . : 2012年9月1日 上午 06:30:38
                                              //两者差距6小时
```

# 12.3 配置保留IP地址给特定计算机

DHCP服务器配置IP地址池后，不管哪一台计算机请求获取IP地址，DHCP服务器都会依次把IP地址分配给每一台计算机，如果网段内有固定服务的主机，那就必须给予固定的IP地址，这时候若不将IP地址保留下来，则会发生两台主机IP地址冲突的情况，那两台主机则无法连接，所以必须要配置保留IP地址，下面介绍如何将保留IP地址分配给特定的计算机，首先要确定该计算机的网卡MAC地址，然后把网卡MAC地址和保留的IP地址绑定在一起，由于网卡的MAC地址是独一无二的，所以将它当作标识符，就不会发生IP地址重复的问题了。

## 配置保留IP地址

此例将一个IP地址保留给特定的计算机，所需数据如下表所示。

| | |
|---|---|
| 保留的 IP 地址 | 192.168.233.50 |
| 计算机网卡 MAC 地址 | 00:0C:29:E6:79:44 |

编辑DHCP配置文件，在配置项中添加保留IP地址及计算机网卡MAC地址。

```
[root@localhost ~]# vi /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
#
# create new
# specify domain name
subnet 192.168.233.0 netmask 255.255.255.0 {
        option routers                  192.168.233.1;
        option subnet-mask              255.255.255.0;
        option domain-name              "jerryit.idv.cn";
        option domain-name-servers      168.95.1.1,192.168.233.1;
        range 192.168.233.10 192.168.233.99;
        host ns {
                hardware ethernet 00:0C:29:E6:79:44;      //指定网卡MAC
                fixed-address 192.168.233.50;             //保留的IP地址
        }
}
```

配置完成后，必须重新启动DHCP服务器服务，配置才会生效。

```
[root@localhost ~]# service dhcpd restart
Shutting down dhcpd:                                        [  OK  ]
Starting dhcpd:                                             [  OK  ]
```

## 客户端测试

在特定计算机的命令控制台中，输入【ipconfig/renew】，再次向DHCP 服务器重新获取IP地址，获取IP地址后，输入【ipconfig/all】，检查是否是所配置的保留IP地址。

```
Windows IP Configuration
        Host Name . . . . . . . . . . . . : user-3d0c157d5a
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : jerryit.idv.cn

Ethernet adapter 本地连接 2:
        Connection-specific DNS Suffix  . : jerryit.idv.cn
        Description . . . . . . . . . . . : AMD PCNET Family PCI Ethernet Adapter #2
        Physical Address. . . . . . . . . : 00-0C-29-E6-79-44
                                           //指定的网卡 MAC 地址
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.233.50
                                          //所保留的 IP 地址
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.233.1
        DHCP Server . . . . . . . . . . . : 192.168.233.195
        DNS Servers . . . . . . . . . . . : 168.95.1.1
                                            192.168.233.1
        Lease Obtained. . . . . . . . . . : 2012 年 8 月 31 日  下午 11:53:31
        Lease Expires . . . . . . . . . . : 2012 年 9 月 1 日  上午 11:53:31
```

# 第13章

# SSH——远程连接服务器

SSH是Secure Shell的缩写，由IETF的网络工作小组（Network Working Group）所制定，SSH是建立在应用层和传输层上的安全协议。

传统的网络服务程序，如FTP、POP和Telnet本身其实都是不安全的，因为它们在网络上使用明文传送数据，数据很容易被截获。而SSH是目前比较可靠的协议，专为远程登录会话和其他网络服务提供安全性。利用SSH协议可以有效防止远程管理过程中的信息泄漏问题。通过SSH可以对所有传输的数据进行加密，也能够防止DNS欺骗和IP地址欺骗。

SSH还有一个额外的优点，即传输的数据是经过压缩的，所以可以加快传输的速度。SSH有很多功能，它既可以代替Telnet，也可提供一个安全的通道。

CentOS系统默认在安装好操作系统后就已经安装了SSH服务，也将它配置为默认启动，所以无需安装。

## 13.1 允许特定用户登录

CentOS系统服务主机内已默认创建了多个用户，如果每个用户都可以利用SSH登录，那就降低了服务器的安全性，虽然不是每个用户都拥有管理员权限，但是这样做还是会增加服务器的风险性。为了降低服务器风险，必须限制哪些用户可以利用SSH登录。

### 配置特定用户登录

若要配置特定用户才可以利用SSH登录服务器，则需要在SSH配置文件的最后一行增加允许登录的用户信息。下面的示例中配置账号tom可以登录，其他账号都不可以利用SSH登录服务器，配置后保存退出，若允许多个用户登录，则在此行后面继续添加其他用户信息。

```
[root@localhost ~]# vi /etc/ssh/sshd_config
AllowUsers tom                                          //允许 tom 用户可以登录
```

配置允许特定用户登录后，必须重新启动ssh服务，配置才会生效。

```
[root@localhost ~]# service sshd restart
Stopping sshd:                                                   [  OK  ]
Starting sshd:                                                   [  OK  ]
```

## 特定用户登录测试

以tom用户登录测试，如果可以正常登录，其他用户无法登录，说明配置成功。特定用户登录后，再用su命令切换到root用户操作，这样风险性也比较低。

```
login as: tom
tom@192.168.233.200's password: *********
[tom@localhost ~]$ su root
Password:
[root@localhost tom]#
```

使用没有配置的jerry用户登录，输入密码后，显示警告信息Access denied（拒绝登录），连续输入5次密码后就会关闭连接。

```
login as: jerry
jerry@192.168.233.200's password: *********
Access denied
jerry@192.168.233.200's password:
```

CentOS系统中root用户管理权限最大，假如root用户的密码被别人知道，再利用系统默认开启的SSH服务登录系统，系统就无安全性可言，所以必须设置SSH服务中禁止以root用户登录，这样要使用root用户就必须在本机登录。

# 13.2 禁止root用户登录

在CentOS操作系统中，管理员root用户权限就相当于Windows操作系统的Administrator，因为SSH服务默认可以使用root用户登录，提高了系统的风险性，所以建议禁止root用户利用SSH服务登录。如果普通用户要对系统进行操作，可以利用su命令切换到root账号，这样可以以root用户权限进行操作，虽然此做法可以降低系统风险性，但是其他用户也知道了root用户的密码，系统就等于公开了，如果只知道普通用户的密码，就算他登录后，还是需要有更高的权限才可以修改，虽然不能说很安全，但是多一套防御总是好的。

## 配置root用户禁止登录

SSH服务默认可以让root用户登录，如果要禁止root用户登录，必须修改SSH配置文件，把PermitRootLogin的yes改成no，将#号删除，修改完成后保存退出。

```
[root@localhost ~]# vi  /etc/ssh/sshd_config
```

```
PermitRootLogin no                //默认为 yes，禁止则设为 no，删除#号
```

修改SSH配置文件后，必须重新启动SSH服务，配置才会生效。

```
[root@localhost ~]# service sshd restart
Stopping sshd:                                              [  OK  ]
Starting sshd:                                              [  OK  ]
```

## 禁止root用户登录测试

开启 PieTTY，输入登录用户名 root，会出现警告信息 Access denied（拒绝访问）。

```
login as: root
root@192.168.233.200's password: *********
Access denied
root@192.168.233.200's password:
```

# 13.3 配置指定网卡接收SSH客户端连接

若要指定网卡接收SSH连接，就需要用户知道SSH服务监听哪块网卡，如eth0、eth1，只有知道了网卡配置的IP地址才可以登录，这样也可以降低服务器的风险性，还可以将SSH服务流量集中在同一块网卡上，避免传输数据时影响服务器的其他服务，缺点是网卡发生硬件故障时，就必须到服务器本机重新配置指定网卡。

## 配置指定网卡接收SSH客户端连接

配置指定网卡接收SSH客户端连接，其实就是在那块指定的网卡上监听SSH服务，利用网卡的IP地址进行配置，下面的示例中利用两块网卡作为示范。

| | |
|---|---|
| eth0 网卡 IP 地址 | 192.168.233.200 |
| eth1 网卡 IP 地址 | 192.168.233.201 |

首先检查服务器IP地址配置。

```
[root@localhost ~]# ifconfig
eth0 Link encap:Ethernet  HWaddr 00:0C:29:91:5F:2E
      inet addr:192.168.233.200  Bcast:192.168.233.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fe91:5f2e/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:207 errors:0 dropped:0 overruns:0 frame:0
      TX packets:112 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:18814 (18.3 KiB)  TX bytes:9473 (9.2 KiB)
eth1 Link encap:Ethernet  HWaddr 00:0C:29:91:5F:38
      inet addr:192.168.233.201  Bcast:192.168.233.255  Mask:255.255.255.0
```

```
        inet6 addr: fe80::20c:29ff:fe91:5f38/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:27 errors:0 dropped:0 overruns:0 frame:0
        TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:2609 (2.5 KiB)  TX bytes:636 (636.0 b)
```

编辑SSH配置文件，参数ListenAddress默认不启用，配置可以接收客户端连接SSH服务器的IP地址，必须将ListenAddress前面的#号删除，再将0.0.0.0改成指定的IP地址，这里允许IP地址为192.168.233.200的ech0网卡接收SSH客户端连接，修改完后保存退出。

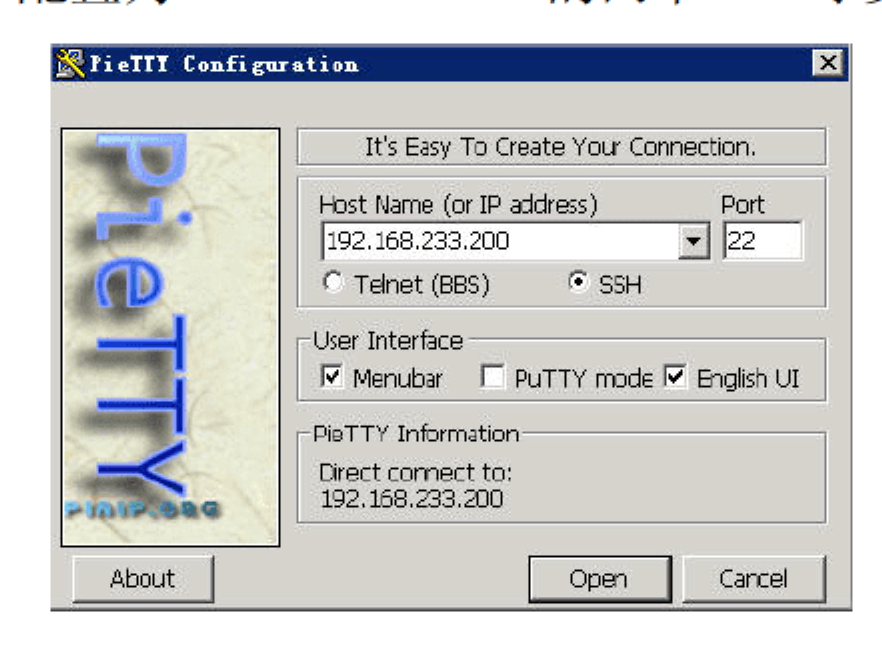
```
[root@localhost ~]# vi /etc/ssh/sshd_config
ListenAddress 192.168.233.200        //默认为 0.0.0.0，配置指定的 IP 地址
```

修改SSH配置文件后，必须重新启动SSH服务，这样配置才会生效。

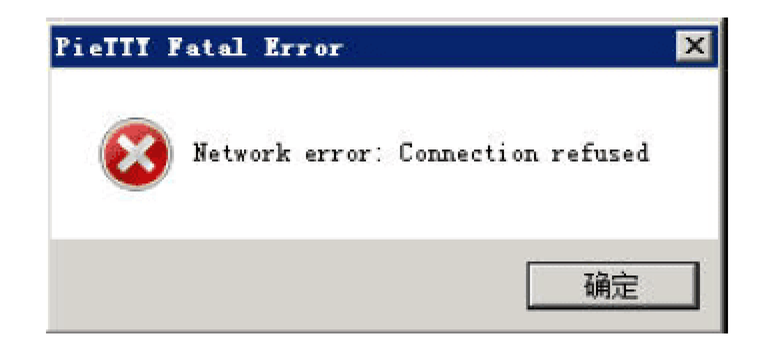
```
[root@localhost ~]# service sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
```

## 指定网卡接收SSH客户端连接测试

使用PieTTY登录测试，配置为192.168.233.200的网卡eth0可以登录。




再来测试网卡eth1，因为该网卡配置IP地址为192.168.233.201，登录时会出现Network error：Connection refused，这样代表配置成功。




# 13.4 配置输入密码时间过长即断开连接

配置输入密码时间过长即断开连接，虽然没有多大的意义，只是为了SSH服务器登录时，时间过长不输入账号密码即断开连接，可以减少不必要的连接。

### 配置等待时间

SSH服务器默认输入密码等待时间过长即断开连接的时间为2分钟，可以自行修改等待时间，例如等待30秒即断开连接，编辑SSH配置文件，将等待时间改成30s，并将#号删除。

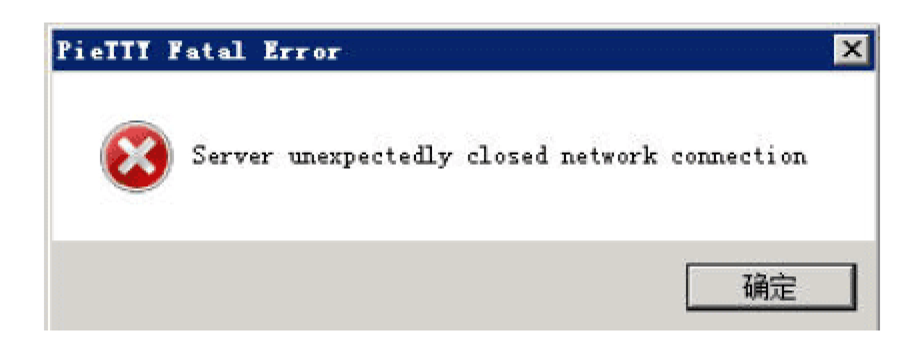
```
[root@localhost ~]# vi /etc/ssh/sshd_config
LoginGraceTime 30s                                          //配置等待时间
```

修改配置文件后，必须重新启动SSH服务，这样配置才会生效。

```
[root@localhost ~]# service sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
```

### 测试等待时间

打开PieTTY输入IP地址后，等待30秒不做任何动作，就会出现错误信息Server unexpectedly closed network connection，然后断开SSH服务连接。




## 13.5 配置空闲时间关闭连接

使用SSH连接一段时间后，空闲时间太久没有任何动作或者忘记关闭PieTTY软件，SSH服务器就会将连接关闭，这样可以节省主机资源。

### 配置空闲时间

在SSH配置文件中，ClientAliveInterval参数代表关闭连接的秒数，ClientAliveCountMax参数代表允许超时的次数。这里将ClientAliveInterval参数设为10秒，将ClientAliveCountMax参数设成0。

```
[root@localhost /]# vi  /etc/ssh/sshd_config
ClientAliveInterval 10    //默认为 0 不启用，启用要删除#号配置秒数
ClientAliveCountMax 0     //默认为 3 不启用，启用要删除#配置次数
```

修改过配置文件后，必须重新启动SSH服务，这样配置才会生效。

```
[root@localhost ~]# service sshd restart
Stopping sshd:                                             [  OK  ]
```

```
Starting sshd:                                             [  OK  ]
```

## 空闲时间关闭连接测试

空闲时间的配置值，需要在新打开的PieTTY连接中生效，如果是以前打开的PieTTY连接就不会关闭。打开新的PieTTY登录后，不要做任何动作，10秒过后就会由于空闲时间过长而关闭连接。




目前测试过的环境，有些版本配置了ClientAliveCountMax的次数，那么配置就不会生效，要将之设成0，就可以正常使用。有些参考文档说明SSH服务空闲关闭是由ClientAliveCountMax配置的，不过这一行是次数而不是秒数，有些参考文档说配置秒数即可，这是比较令人疑惑的地方。还有一些参考文档说明配置ClientAliveInterval秒数就会生效，不过测试过所有做法，目前只有上述配置是成功的，或许版本不一样会有所差异。

# 第 14 章

# Telnet——远程登录服务器

Telnet是Internet远程登录服务的标准协议，此协议的历史非常悠久，应用最广泛的就是BBS服务，传统的Telnet连接对话所传输的数据没有加密，所有输入及显示的数据，包括最重要的用户名及密码都是明文显示，这样会增加服务器的风险性，因此近几年来有许多操作系统默认不安装此协议，而改用更为安全的SSH服务。Microsoft Windows从Vista开始，不再安装Telnet客户端，需要手动安装。而之前的版本，只要计算机启动了TCP/IP服务，Telnet就可以使用。

## 14.1 安装Telnet 服务器

下面介绍如何配置简单的Telnet服务器。

### 检查Telnet软件

检查是否已安装Telnet 服务器软件，默认不安装。配置Telnet Server所需的软件为xinetd及telnet-server：

```
[root@localhost /]# rpm -qa | grep xinetd
xinetd-2.3.14-29.el6.x86_64
[root@localhost /]# rpm  -qa | grep telnet-server
telnet-server-0.17-46.el6.x86_64
```

### 安装Telnet 服务

如果要安装Telnet Server，使用yum在线更新方式安装，既方便又简单。若只使用telnet client工具，即可输入【yum install -y telnet-server】。

```
[root@localhost ~]# yum install  -y telnet-server
Dependencies Resolved
========================================================================
```

```
 Package           Arch         Version                   Repository   Size
==========================================================================
Installing:
 telnet-server     x86_64       1:0.17-46.el6             base          36 k
Installing for dependencies:
 xinetd            x86_64       2:2.3.14-29.el6           base         120 k
Transaction Summary
==========================================================================
Install       2 Package(s)
Upgrade       0 Package(s)
Total download size: 157 k
```

## 配置Telnet服务

在启动Telnet Server服务前，必须修改Telnet配置文件，因为disable参数默认为yes，表示Telnet Server禁止连接，所以必须修改为no。

```
[root@localhost /]# vi /etc/xinetd.d/telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags             = REUSE
        socket_type       = stream
        wait              = no
        user              = root
        server            = /usr/sbin/in.telnetd
        log_on_failure   += USERID
        disable           = no    //默认为 yes 禁止连接，必须设为 no 才可以允许连接
```

## 启动Telnet 服务

配置完成后，就可以启动Telnet服务了，若有需要应将xinetd服务设为默认启动。

```
[root@localhost ~]# service xinetd start
Starting xinetd:                                             [  OK  ]
[root@localhost ~]# chkconfig xinetd on
```

说明

Telnet Server服务依赖于xinetd超级服务。

检查Telnet Server端口是否监听。

```
[root@localhost /]# netstat  -tunlp | grep xinetd
```

```
tcp        0      0 :::23                       :::*                LISTEN      4290/xinetd
```

## 配置防火墙

启动Telnet 服务后，必须在防火墙配置文件中开启23端口，这样Telnet客户端才可以连接进来。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
                                                    //Telnet Server 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

修改防火墙后，必须重新启动防火墙服务，否则配置无法生效。

```
[root@localhost /]# service iptables restart
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

## 测试连接Telnet服务器

Root用户默认不能登录Telnet Server，必须用其他用户登录，使用su命令切换到root用户，建立测试用户jerry，使用Windows操作系统的命令控制台测试，出现信息提示后，输入用户名和密码，若显示如下信息代表可以正常登录。

```
C:\Users\jerry>telnet 192.168.233.200
CentOS Linux release 6.0 (Final)
Kernel 2.6.32-71.el6.x86_64 on an x86_64
login: jerry
Password:
Last login: Mon Aug 22 10:13:01 from 192.168.233.100
[jerry@localhost ~]$
```

# 14.2 修改Telnet 服务端口

Telnet 服务既然被视为是不安全的服务，就要想办法提高其安全性，除了做一些限制外，最常见的方法就是修改端口。

## 修改Telnet 服务端口

编辑services配置文件，默认Telnet Server端口为23，这里将端口修改为2323，然后保存退出。

```
[root@localhost /]# vi /etc/services
telnet          2323/tcp        //默认为 TCP 23
telnet          2323/udp        //默认为 UDP 23
```

修改Telnet 服务端口后，必须重新启动xinetd服务，配置才会生效。

```
[root@localhost /]# service xinetd restart
Stopping xinetd:                                           [  OK  ]
Starting xinetd:                                           [  OK  ]
```

检查修改后的Telnet 服务端口是否为2323，信息显示端口为2323，代表修改成功。

```
[root@localhost /]# netstat  -tunlp | grep xinetd
tcp      0     0 :::2323             :::*              LISTEN      4534/xinetd
```

## 配置防火墙

修改Telnet 服务端口后，也必须修改防火墙配置的连接端口，否则客户端无法连接。

```
[root@localhost /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 2323 -j ACCEPT
                                           //修改后的 telnet 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙修改完毕后，必须重新启动防火墙，配置才会生效。

```
[root@localhost /]# service iptables restart
iptables: Flushing firewall rules:                          [  OK  ]
iptables: Setting chains to policy ACCEPT: filter           [  OK  ]
iptables: Unloading modules:                                [  OK  ]
iptables: Applying firewall rules:                          [  OK  ]
```

## 测试Telnet 服务新端口

使用Windows操作系统测试连接，端口使用2323，若输入用户名和密码可以登录，则代表Telnet Server修改端口成功。

```
C:\Users\jerry>telnet 192.168.233.200 2323
CentOS Linux release 6.0 (Final)
Kernel 2.6.32-71.el6.x86_64 on an x86_64
login: jerry
Password:
Last login: Mon Aug 22 10:19:58 from 192.168.233.100
[jerry@localhost ~]$
```

# 14.3 配置连接IP地址及连接时间

Telnet Server如果要管理Telnet Client连接时间，就要使用access_times参数限制用户连接时间，并且一定要配合限制的主机条件，如限制IP地址或网段，这样比较安全。

这里限制IP地址为192.168.233.100，该IP地址只能在每天10:00~12:00及20:00~23:45可以登录Telnet Server，其他时间禁止连接。假设Telnet Server主机开放到23:45，但是客户端时间只到23:40，那就算Telnet Server主机时间已到，客户端还是可以登录的。

```
[root@localhost /]# vi /etc/xinetd.d/telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags              = REUSE
        socket_type        = stream
        wait               = no
        user               = root
        server             = /usr/sbin/in.telnetd
        log_on_failure   += USERID
        disable            = no
        only_from = 192.168.233.100                    //允许的 IP 地址
        access_times = 10:00-12:00 20:00-23:45         //允许的连接时间
}
```

Telnet Server配置完成后保存退出，重新启动xinetd服务，配置才会生效。

```
[root@localhost /]# service xinetd restart
Stopping xinetd:                                            [  OK  ]
Starting xinetd:                                            [  OK  ]
```

## 14.4 配置Telnet Server连接数

Telnet Server配置连接数，就是配置服务器允许几个连接，服务器上的服务连接数过高，会影响服务器的效率，所以要限制连接数，这样不会浪费资源，不然很多连接都挂在服务器上没有断线。如果服务器没有自动断线的限制，就会影响主机的效率。

编辑Telnet Server配置文件，将instances参数设为2，默认没有这一行，需要自行添加。Telnet Server大约在两个连接后，就会无法登录，有时到3个才会禁止连接，这一点控制得不是很准确。

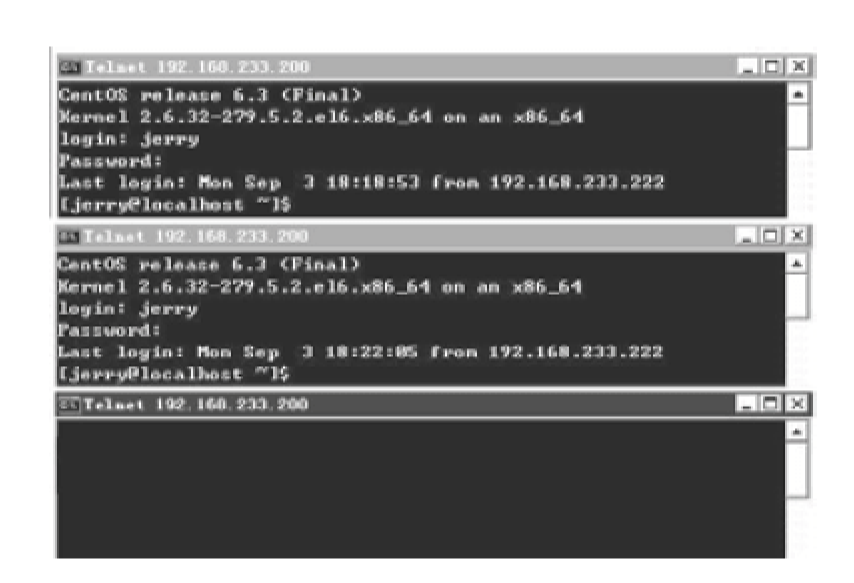
```
[root@localhost /]# vi /etc/xinetd.d/telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure   += USERID
        disable         = no
        instances = 2                              //默认没有这一行，自行添加
}
```

Telnet Server修改配置后，必须重新启动xinetd服务，配置才会生效。

```
[root@localhost /]# service xinetd restart
Stopping xinetd:                                            [  OK  ]
Starting xinetd:                                            [  OK  ]
```

### 测试连接数

使用Windows系统的命令控制台测试连接，连续登录，第三次登录就不会出现输入用户名和密码的界面。




# 14.5 配置特定IP地址或网段登录

配置特定IP地址可以登录Telnet Server，这样不仅可以增加Telnet Server的安全性，也可以知道有哪些客户端登录到Telnet Server上，以便对Telnet Client进行有效地连接管理。

## 配置单一IP地址登录

这里配置只有192.168.233.100可以登录Telnet Server，其他主机不可以登录，编辑Telnet Server配置文件，配置参数only_from，添加允许登录的IP地址。

```
[root@localhost /]# vi /etc/xinetd.d/telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = no
        only_from = 192.168.233.100           //只允许 192.168.233.100 登录
}
```

编辑Telnet Server配置文件后，必须重新启动xinetd服务，配置才会生效。

```
[root@localhost /]# service xinetd restart
Stopping xinetd:                                           [  OK  ]
Starting xinetd:                                           [  OK  ]
```

在192.168.233.100客户端使用命令控制台登录，可以正常登录，代表配置成功，其他客户端则无法登录。

```
C:\Users\jerry>telnet 192.168.233.200
CentOS Linux release 6.0 (Final)
Kernel 2.6.32-71.el6.x86_64 on an x86_64
login: jerry
Password:
```

```
Last login: Mon Aug 22 10:45:50 from 192.168.233.100
[jerry@localhost ~]$
```

## 配置特定网段登录

配置192.168.9.0/24的网段都可以登录，其他网段都不可以登录，在only_from 参数上增加允许登录的网段。

```
[root@localhost /]# vi /etc/xinetd.d/telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = no
        only_from=192.168.9.0/24           //限制只有 192.168.9.0/24 网段才可以登录
}
```

编辑Telnet Server配置文件后，必须重新启动xinetd服务，配置才会生效。

```
[root@localhost /]# service xinetd restart
Stopping xinetd:                                          [  OK  ]
Starting xinetd:                                          [  OK  ]
```

## 配置网段内特定IP不可登录

开放特定的网段连接，有时会限制其中几个IP地址不可以连接，所以必须要排除不可连接的IP地址，例如，配置192.168.9.100及192.168.9.200不可以登录，其他192.168.9.0/24网段都可以登录。

编辑Telnet Server配置文件，除了原本的允许网段外，在no_access参数中添加IP地址192.168.9.{100,200}。

```
[root@localhost /]# vi /etc/xinetd.d/telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags            = REUSE
        socket_type      = stream
        wait             = no
        user             = root
```

```
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = no
        only_from=192.168.9.0/24            //限制只有 192.168.9.0/24 网段才可以登录
        no_access=192.168.9.{100,200}
                                    //此网段中 192.168.9.100 和 200 配置无法登录
}
```

编辑Telnet Server配置文件后，必须重新启动xinetd服务，配置才会生效。

```
[root@localhost /]# service xinetd restart
Stopping xinetd:                                            [  OK  ]
Starting xinetd:                                            [  OK  ]
```

# 14.6 配置允许root用户登录

在CentOS操作系统下，系统管理员root用户权限相当于Windows的administrator，所以Telnet Server可以让root用户登录是安全性的一大隐患，建议禁止该用户，若要开放，建议可以配置特定IP地址或网段登录。

## 开放root用户登录

开放root用户登录的方法很简单，只要将securetty更换为其他名称，这样系统就读不到securetty文件，则不会限制root用户登录。

```
[root@localhost /]# mv  /etc/securetty  /etc/securetty.bk
```

修改配置后，必须重新启动xinetd服务，配置才会生效。

```
[root@localhost /]# service xinetd restart
Stopping xinetd:                                            [  OK  ]
Starting xinetd:                                            [  OK  ]
```

## root用户登录测试

在客户端使用root用户登录Telnet Server，若可以正常登录，代表配置成功。

```
C:\Users\jerry>telnet 192.168.233.200
CentOS Linux release 6.0 (Final)
Kernel 2.6.32-71.el6.x86_64 on an x86_64
login: root                     //root 登录
Password:
Last login: Mon Aug 22 09:02:29 from 192.168.233.100
[root@localhost ~]#
```

# 第 15 章

# YUM——在线更新服务器

假设公司内有很多CentOS系统主机，如果每台都对外更新软件，则公司的网络带宽就会下降，更何况更新的站点不一定是速度最快的。有些人建议使用光盘更新，但是光盘内的软件不一定是最新版本，那么有什么方法可以让更新速度最快、软件版本最新呢？方法就是自行配置在线更新服务器，其一局域网的速度一定是最快的，其二在线更新服务器会下载一份软件的最新版本，若每一台CentOS主机都使用在线更新服务器的话，不仅可以节省公司网络带宽，也可以保证软件永远是最新的。

## 15.1 配置在线更新服务器

下面介绍如何配置在线更新服务器，以提供公司内部环境更新，节省公司网络带宽。

### 安装mirrordir软件

CentOS系统默认没有安装mirrordir软件，安装mirrordir软件需要两个RPM文件，分别为mirrordir-devel、mirrordir（缺一不可），首先使用wget方式下载，然后再安装。

```
[root@localhost ~]# wget
http://pkgs.repoforge.org/mirrordir/mirrordir-0.10.49-1.2.el5.rf.x86_64.rpm
[root@localhost ~]# wget
http://pkgs.repoforge.org/mirrordir/mirrordir-devel-0.10.49-1.2.el5.rf.x86_64.rpm
                                                    //mirrordir 软件下载
```

> 说明
>
> 数据来源：http://pkgs.repoforge.org/mirrordir/。

两个RPM文件必须一起安装，否则安装时会发生错误。

```
[root@localhost ~]# rpm -ivh mirrordir*     //mirrordir 软件安装
warning: mirrordir-0.10.49-1.2.el5.rf.x86_64.rpm: Header V3 DSA/SHA1 Signature, key ID
6b8d79e6: NOKEY
Preparing...            ########################################### [100%]
   1:mirrordir          ########################################### [ 50%]
   2:mirrordir-devel    ########################################### [100%]
```

## 安装yum-arch 软件

安装YUM在线更新服务器还需要yum-arch软件，该软件的功能是分析 RPM 软件的header，CentOS 6.x操作系统必须安装2.2.2-9版，否则无法安装成功。

```
[root@localhost ~]# wget
ftp://fr2.rpmfind.net/linux/epel/beta/6/i386/yum-arch-2.2.2-9.el6.noarch.rpm
                                                       //下载 yum-arch
[root@localhost ~]# rpm -ivh yum-arch*                 //安装 yum-arch
warning: yum-arch-2.2.2-9.el6.noarch.rpm: Header V3 RSA/SHA256 Signature, key ID 0608b895:
NOKEY
Preparing...            ########################################### [100%]
   1:yum-arch           ########################################### [100%]
```

> **说明**
>
> 文件来源：http://rpmfind.net/linux/RPM/epel/beta/6/i386/yum-arch-2.2.2-9.el6.noarch.html。

## 下载并安装createrepo 软件

安装YUM在线更新服务器还需要createrepo软件，该软件主要功能是建立索引文件，可以使用YUM在线更新方式下载安装。

```
[root@localhost ~]# yum install -y createrepo
Dependencies Resolved
=========================================================================
 Package          Arch          Version                Repository    Size
=========================================================================
Installing:
 createrepo    noarch     0.9.8-4.el6                  base           81 k
Installing for dependencies:
 deltarpm          x86_64  3.5-0.5.20090913git.el6     base           71 k
 python-deltarpm   x86_64  3.5-0.5.20090913git.el6     base           27 k
Transaction Summary
=========================================================================
Install       3 Package(s)
Upgrade       0 Package(s)
Total download size: 179 k
```

## 配置安装Apache服务

在线更新服务器配置方法会用到Apache服务，所以必须安装Apache服务。

```
[root@localhost ~]# yum install -y httpd
Dependencies Resolved
Package          Arch        Version              Repository          Size
========================================================================
Installing:
 httpd           x86_64       2.2.15-5.el6.centos    base           811 k
Installing for dependencies:
 apr             x86_64      1.3.9-3.el6_0.1        updates        124 k
 apr-util        x86_64      1.3.9-3.el6_0.1        updates        87 k
 apr-util-ldap   x86_64      1.3.9-3.el6_0.1        updates        15 k
 httpd-tools     x86_64      2.2.15-5.el6.centos    base           68 k
Transaction Summary
===========================================================
Install       5 Package(s)
Upgrade       0 Package(s)
Total download size: 1.1 M
```

CentOS 6.x的Apache启动时，会出现ServerName警告信息，只要编辑Apache配置文件，将ServerName前面的#号删除，这样启动Apache就不会发生警告了。

```
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.  See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
ServerName www.example.com:80                            //将#号删除即可
```

设置Apache配置文件后，就可以启动Apache了，在线更新服务器是长久使用的服务，所以将Apache服务配置为默认启动。

```
[root@localhost ~]# service httpd start
Starting httpd:                                            [  OK  ]
[root@localhost ~]# chkconfig httpd on
```

## 配置防火墙

配置在线更新服务器需要使用Apache服务，所以必须在防火墙中开启Apache端口80。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完毕后，必须重新启动防火墙，否则配置不会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

## 创建在线更新服务器软件目录

必备软件安装完毕后，就要创建软件的存放目录，这里使用CentOS 6.0的x86_64环境，所以在Apache网页目录中依次建立os、updates、extras三个目录。

```
[root@localhost ~]# mkdir -p /var/www/html/yum/centos/6/os/x86_64
[root@localhost ~]# mkdir -p /var/www/html/yum/centos/6/updates/x86_64
[root@localhost ~]# mkdir -p /var/www/html/yum/centos/6/extras/x86_64
```

**说明**

建立目录加上参数p，功能为直接建立所有相关目录。

## 下载在线更新服务器软件

将所有更新软件下载到在线更新服务器内，光x86_64就有近8GB，下载时间有点久，以50MB/s光纤的速度下载，也要花一个多小时，可以泡杯咖啡慢慢等。依次输入命令下载软件，建议同时开启3个PuTTY连接，不然第一个命令下载完后，再回来输入第二个命令，既费时又麻烦，尤其是第一个与第二个命令下载的软件较多。

```
[root@localhost ~]# mirrordir -v ftp://ftp.nsysu.edu.tw//Unix-like/CentOS/6.0/os/x86_64
/var/www/html/yum/centos/6/os/x86_64
…中间省略…
[root@localhost ~]# mirrordir -v
ftp://ftp.nsysu.edu.tw/Unix-like/CentOS/6.0/updates/x86_64
/var/www/html/yum/centos/6/updates/x86_64
…中间省略…
[root@localhost ~]# mirrordir -v
ftp://ftp.nsysu.edu.tw/Unix-like/CentOS/6.0/extras/x86_64
/var/www/html/yum/centos/6/extras/x86_64
…中间省略…
```

测试过多个大学的站点，目前只有中国台湾中山大学的FTP站台可以完整下载，义守大学的FTP站点有时下载到一半就停住，所以若遇到下载到一半就停止不动的情况，只能停用网络再启用网络，这样才能把软件下载完整。

## 分析 RPM 软件的 header

使用yum-arch分析 RPM 软件的 header，依次分析os、updates、extras三个目录，若此软件版本不符合，CentOS 6.0操作系统就会发生错误。

```
[root@localhost ~]# yum-arch /var/www/html/yum/centos/6/os/x86_64
THIS PROGRAM IS DEPRECATED!
You should be generating xml metadata instead.
Please see http://linux.duke.edu/metadata
Digesting rpms 21 % complete:
jakarta-commons-collections-testframework-3.2.1-3.4.el6.noarDigesting rpms 23 %
complete: tigervnc-server-applet-1.0.90-0.10.20100115svn3945.el6.noarcDigesting rpms 28
% complete: geoclue-devel-0.11.1.1-0.13.20091026git73b6729.el6.x86_64.rpDigesting rpms
29 % complete: mobile-broadband-provider-info-devel-1.20100122-1.el6.noarchDigesting
rpms 35 % complete:
gstreamer-plugins-bad-free-devel-docs-0.10.19-2.el6.x86_64.rDigesting rpms 36 %
complete: jakarta-commons-collections-testframework-javadoc-3.2.1-3.4.Digesting rpms 39
% complete: tigervnc-server-module-1.0.90-0.10.20100115svn3945.el6.x86_6Digesting rpms
42 % complete: xorg-x11-drv-nouveau-0.0.16-8.20100423git13c1043.el6.x86_64.Digesting
rpms 45 % complete:
dbus-c++-devel-0.5.0-0.10.20090203git13281b3.1.el6.x86_64.rpDigesting rpms 50 %
complete: openoffice.org-presentation-minimizer-3.2.1-19.6.el6.x86_64.Digesting rpms 93
% complete: pentaho-reporting-flow-engine-javadoc-0.9.2-5.OOo31.el6.noarDigesting rpms
100 % complete: nss-pkcs11-devel-3.12.7-2.el6.i686.rpm           .rpmmrpm
   Total: 6019
   Used: 6019
   Src: 0
Writing header.info file
[root@localhost ~]# yum-arch /var/www/html/yum/centos/6/updates/x86_64
THIS PROGRAM IS DEPRECATED!
You should be generating xml metadata instead.
Please see http://linux.duke.edu/metadata
Digesting rpms 30 % complete:
openoffice.org-presenter-screen-3.2.1-19.6.el6_0.5.x86_64.rpDigesting rpms 38 %
```

```
complete: openoffice.org-opensymbol-fonts-3.2.1-19.6.el6_0.5.rpDigesting rpms 62
% complete: openoffice.org-presentation-minimizer-3.2.1-19.6.el6_0.5.x86Digesting rpms
100 % complete: qt-devel-4.6.2-17.el6.x86_64.rpm                mrpm4.rpm
   Total: 1042
   Used: 1042
   Src: 0
Writing header.info file
[root@localhost ~]# yum-arch /var/www/html/yum/centos/6/extras/x86_64
THIS PROGRAM IS DEPRECATED!
You should be generating xml metadata instead.
Please see http://linux.duke.edu/metadata
Digesting rpms 100 % complete: centos-release-cr-6-0.el6.centos.x86_64.rpm
   Total: 1
   Used: 1
   Src: 0
Writing header.info file
```

此错误为yum-arch软件版本不符，更换至对应的版本即可。

```
[root@localhost ~]# yum-arch /var/www/html/yum/centos/6/os/x86_64
Traceback (most recent call last):
  File "/usr/bin/yum-arch", line 22, in <module>
    import pullheaders
  File "/usr/share/yum-arch/pullheaders.py", line 27, in <module>
    from yum.logger import Logger
  File "/usr/share/yum-arch/yum/__init__.py", line 908
    self.repos.populateSack (with='filelists')
                              ^
SyntaxError: invalid syntax
```

## createrepo建立索引文件

Createrepo 软件会自动产生 XML metadata，在目录下产生 repodata 文件夹，依次分析os、updates、extras三个目录。

```
[root@localhost ~]# createrepo /var/www/html/yum/centos/6/os/x86_64
4786/6019 - Packages/slang-2.2.1-1.el6.i686.rpm
iso-8859-1 encoding on Ville Skytt▒ <ville.skytta@iki.fi> - 2.8.2-2
6019/6019 - Packages/nss-pkcs11-devel-3.12.7-2.el6.i686.rpm
Saving Primary metadata
Saving file lists metadata
Saving other metadata
[root@localhost ~]# createrepo /var/www/html/yum/centos/6/updates/x86_64
 860/1042 - RPMS/pango-devel-1.28.1-3.el6_0.3.i686.rpm
iso-8859-1 encoding on Ville Skytt▒ <ville.skytta@iki.fi> - 2.8.2-2
1042/1042 - RPMS/qt-devel-4.6.2-17.el6.x86_64.rpm
Saving Primary metadata
Saving file lists metadata
Saving other metadata
[root@localhost ~]# createrepo /var/www/html/yum/centos/6/extras/x86_64
1/1 - RPMS/centos-release-cr-6-0.el6.centos.x86_64.rpm
Saving Primary metadata
Saving file lists metadata
Saving other metadata
```

软件每个月多少都会更新，建议每个月更新一次，不过更新不大，可以创建计划任务或shell脚本去执行，不然要执行太多行的命令。

## 客户端进行repo配置

在线更新服务器配置后，接下来就是配置客户端的repo，将base、updates、extras三个目录的mirrorlist加上#，然后修改baseurl路径，将http://mirror.centos.org/centos这一段修改成http://192.168.233.192/yum/centos，修改完毕后，保存退出，这样客户端就可以使用所配置的在线更新服务器更新软件了。

```
[root@localhost ~]# cd /etc/yum.repos.d
[root@localhost yum.repos.d]# cp CentOS-Base.repo CentOS-Base.repo.old
                                        //将内建的 CentOS-Base.repo 复制一份
[root@localhost yum.repos.d]# vi CentOS-Base.repo          //修改默认 repo
# CentOS-Base.repo
#
# The mirror system uses the connecting IP address of the client and the
# update status of each mirror to pick mirrors that are updated to and
# geographically close to the client.  You should use this for CentOS updates
# unless you are manually picking other mirrors.
#
# If the mirrorlist= does not work for you, as a fall back you can try the
# remarked out baseurl= line instead.
#
#
[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os
baseurl=http://192.168.233.192/yum/centos/$releasever/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=upda
tes
baseurl=http://192.168.233.192/yum/centos/$releasever/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extr
as
baseurl=http://192.168.233.192/yum/centos/$releasever/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
```

说明

192.168.233.192为示例IP地址。

## 15.2 使用光盘安装更新软件

CentOS操作系统运行时，如果遇到主机配置不能连接广域网的话，在需要安装软件时，YUM方式就无法安装，其实换一种方式，将数据源由网络改成光盘，就可以使用了，不过有一点要注意，使用光盘做数据源的话，光盘软件的版本不一定是最新版本，所以若有这种顾虑，不建议使用这样的方式。

CentOS系统默认在目录/etc/yum.repos.d下有两个repo文件，CentOS-Base.repo是给在线YUM使用，另一个CentOS-Media.repo是给光盘YUM使用，系统安装完后，只有CentOS-Base.repo是启用的，CentOS-Media.repo是停用的。

假设没有网络时，只能使用光盘来YUM安装软件，那就先到yum.repos.d目录中，编辑CentOS-Media.repo文件，通过baseurl配置光盘路径，这里将光盘挂载到/mnt/cdrom下，将enabled设为1，这样配置才会启动，CentOS-Base.repo就将之改名或者将enabled设为0，建议将配置文件改名，以免日后要使用CentOS-Base.repo文件时出现问题。

```
[root@localhost ~]# cd /etc/yum.repos.d/
[root@localhost yum.repos.d]# mv CentOS-Base.repo CentOS-Base.repo.bk
[root@localhost yum.repos.d]# vi CentOS-Media.repo
# CentOS-Media.repo
#
# This repo is used to mount the default locations for a CDROM / DVD on
#  CentOS-6.  You can use this repo and yum to install items directly off the
#  DVD ISO that we release.
#
# To use this repo, put in your DVD and use it with the other repos too:
#  yum --enablerepo=c6-media [command]
#
# or for ONLY the media repo, do this:
#
#  yum --disablerepo=\* --enablerepo=c6-media [command]

[c6-media]
name=CentOS-$releasever - Media
baseurl=file:///mnt/cdrom
gpgcheck=1
enabled=1                                                  //1 启用，0 停用
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
```

接下来就是挂载光盘到/mnt/cdrom目录，先在/mnt下创建cdrom目录，创建完成后，就可以挂载光盘了，命令如下。

```
[root@localhost ~]# mkdir /mnt/cdrom                    //建立 cdrom 目录
[root@localhost ~]# mount -t iso9660 /dev/cdrom /mnt/cdrom   // 挂载光驱
mount: block device /dev/sr0 is write-protected, mounting read-only
```

光驱挂载成功后，试着安装一个软件，检查Repository是不是c6-media，是的话就代表成功。

```
root@localhost ~]# yum install vsftpd
Loaded plugins: fastestmirror
c6-media                                                      | 4.0 kB     00:00 ...
```

```
c6-media/primary_db                                      | 4.2 MB     00:00 ...
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package vsftpd.x86_64 0:2.2.2-6.el6 set to be updated
--> Finished Dependency Resolution
Dependencies Resolved
========================================================================
 Package         Arch           Version            Repository           Size
========================================================================
Installing:
 vsftpd        x86_64        2.2.2-6.el6           c6-media          149 k
Transaction Summary
========================================================================
Install       1 Package(s)
Upgrade       0 Package(s)
Total download size: 149 k
```

## 永久挂载光驱

接下来无论安装何种软件，安装速度都特别快，不过要长久使用光盘安装，就必须要将光盘挂载信息写入/etc/fstab，这样开机时才可以自动加载。

```
[root@localhost ~]# vi /etc/fstab
#
# /etc/fstab
# Created by anaconda on Sun Sep 18 19:54:12 2012
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/VolGroup-lv_root /                    ext4     defaults        1 1
UUID=371000c0-3dfe-4784-a3a8-677d888248d0 /boot   ext4     defaults        1 2
/dev/mapper/VolGroup-lv_swap swap                 swap     defaults        0 0
tmpfs                   /dev/shm                  tmpfs    defaults        0 0
devpts                  /dev/pts                  devpts   gid=5,mode=620  0 0
sysfs                   /sys                      sysfs    defaults        0 0
proc                    /proc                     proc     defaults        0 0
/dev/cdrom              /mnt/cdrom                iso9660  defaults        0 0
```

# 15.3 指定大学站点

编辑CentOS-Base.repo，将每个mirrorlist前面加上#号停用，然后再将每个baseurl网址修改，这里配置义守大学的文件服务器，配置完成后，清除缓存就可以使用该站点更新软件了。

```
[root@localhost ~]# vi /etc/yum.repos.d/CentOS-Base.repo
# CentOS-Base.repo
#
# The mirror system uses the connecting IP address of the client and the
# update status of each mirror to pick mirrors that are updated to and
# geographically close to the client.  You should use this for CentOS updates
```

```
# unless you are manually picking other mirrors.
#
# If the mirrorlist= does not work for you, as a fall back you can try the
# remarked out baseurl= line instead.
#
#
[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os
baseurl=http://ftp.isu.edu.tw/pub/Linux/CentOS/$releasever/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6

#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=upda
tes
baseurl=http://ftp.isu.edu.tw/pub/Linux/CentOS/$releasever/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extr
as
baseurl=http://ftp.isu.edu.tw/pub/Linux/CentOS/$releasever/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=cent
osplus
baseurl=http://ftp.isu.edu.tw/pub/Linux/CentOS/$releasever/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
#contrib - packages by Centos Users
[contrib]
name=CentOS-$releasever - Contrib
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=cont
rib
baseurl=http://ftp.isu.edu.tw/pub/Linux/CentOS/$releasever/contrib/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
```

# 第16章

# NTP——时间服务器

NTP全名为Network Time Protocol，就是网络时间同步的服务，时间的准确性是非常重要的，很多数据上的记录都需要正确的时间，所以时间不正确时，所记录的数据也不正确。网络上有很多时间的站点，上海交通大学网络中心与中国科学院国家授时中心都配置了时间服务器，所以自行配置的时间服务器都需要与该时间服务器同步。

## 16.1 配置NTP时间服务器

### 检查NTP软件

检查是否安装NTP服务，如果系统没有安装，使用YUM在线更新方式进行安装。CentOS系统默认已安装NTP服务软件。

```
[root@localhost ~]# rpm -qa | grep ntp
ntpdate-4.2.4p8-2.el6.x86_64
fontpackages-filesystem-1.41-1.1.el6.noarch
ntp-4.2.4p8-2.el6.x86_64
```

### 配置同步时间服务器站点

编辑NTP服务配置文件，默认有三个站台数据，全部标上#号，配置5个国内NTP站台的资料。

```
[root@localhost ~]#  vi /etc/ntp.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.rhel.pool.ntp.org           //将原来三组加上#号停用
```

```
#server 1.rhel.pool.ntp.org
#server 2.rhel.pool.ntp.org
server ntp.sjtu.edu.cn     //以下 5 组为国内各大学的时间服务器站点
server s1a.time.edu.cn
server s1b.time.edu.cn
server s1d.time.edu.cn
server s2c.time.edu.cn
```

> 说明
>
> NTP数据来源：http://www.time.ac.cn/links.htm。

## 启动NTP时间服务器

NTP服务配置完成后，在启动NTP服务时，请耐心等待几分钟，本地NTP服务器会与上游时间服务器同步，这样才可以进行时间同步，建议NTP时间服务器是长久运行的服务，将其设为系统默认启动。

```
[root@localhost ~]# service ntpd start        //启动时间服务器
Starting ntpd:                              [  OK  ]
[root@localhost ~]# chkconfig ntpd on      //配置时间服务器默认启动
```

NTP服务启动后，检查当前NTP服务运作的状态。

```
[root@localhost ~]# netstat -tunlp | grep ntpd
udp       0      0 192.168.233.195:123          0.0.0.0:*                      1695/ntpd
udp       0      0 127.0.0.1:123                0.0.0.0:*                      1695/ntpd
udp       0      0 0.0.0.0:123                  0.0.0.0:*                      1695/ntpd
udp       0      0 fe80::20c:29ff:fe46:123      :::*                           1695/ntpd
udp       0      0 ::1:123                      :::*                           1695/ntpd
udp       0      0 :::123                       :::*                           1695/ntpd
```

## 检查时间服务器状态

NTP服务启动完毕后，过几分钟后开始同步，再查询当前NTP时间服务器的时间，刚启动马上查询是不会有任何数据的。

```
[root@localhost ~]# ntpq -p     //检查当前的时间服务器状态
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
210.72.145.44   .INIT.          16 u    -   64    0    0.000    0.000   0.000
 dns.sjtu.edu.cn 114.80.81.13    3 u   13   64    3   30.218    3.292   0.194
 202.112.10.60   .STEP.         16 u   11   64    0    0.000    0.000   0.000
 202.112.7.150   204.235.61.9    3 u    9   64    3    4.181    9.272   0.222
 202.120.23.169  .INIT.         16 u    -   64    0    0.000    0.000   0.000
```

## 配置防火墙

NTP时间服务器配置完成后，要在防火墙配置中开启相对应的端口，否则无法提供其设备的时间同步，时间服务器的端口为UDP 123。

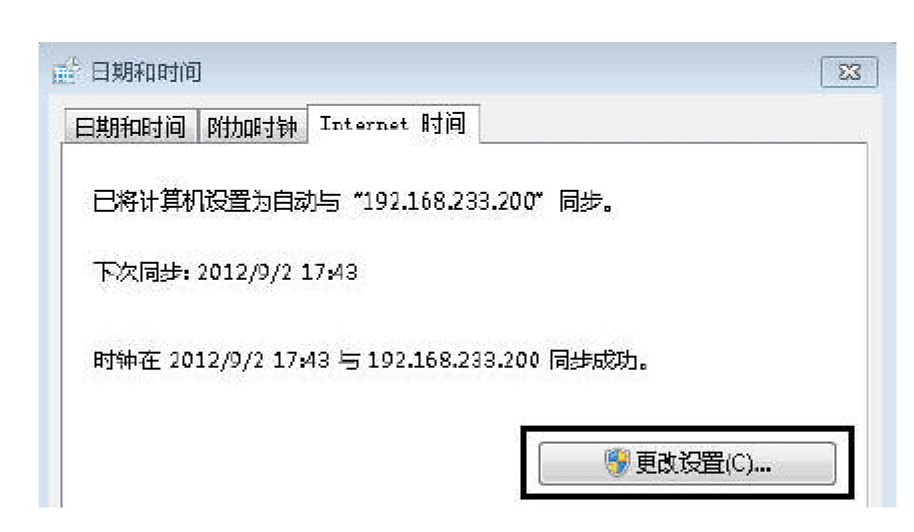
```
 [root@localhost /]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 123 -j ACCEPT
                                                    //NTP 时间服务器端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

配置完防火墙后，必须要重新启动防火墙，否则配置无法生效。

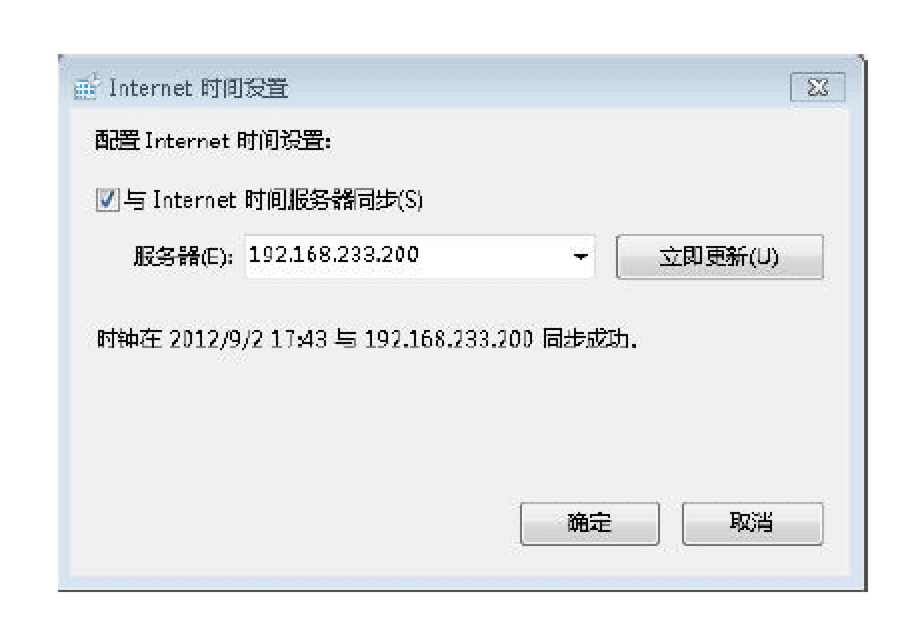
```
[root@localhost /]# service iptables restart
iptables: Flushing firewall rules:                           [  OK  ]
iptables: Setting chains to policy ACCEPT: filter         [  OK  ]
iptables: Unloading modules:                                  [  OK  ]
iptables: Applying firewall rules:                           [  OK  ]
```

## Windows 7客户端时间同步

选择【开始】菜单中的【控制面板】，打开【日期和时间】，选择【Internet时间】，按【更改设置】。




先确认勾选了【与Internet时间服务器同步】，在【服务器】选项中输入NTP服务器的IP地址，然后按【立即更新】，时间就会立即同步。出现完成同步的提示，代表同步成功，也可以将时间调至其他时间，更可以看出是否已正常同步。




## 16.2 调整系统时间及时区

配置完NTP时间服务器后，客户端就要知道该如何同步，以下大致介绍该如何检查时间、调整时间及日期，更重要的是如何将时间写入硬件。

调整系统时间前，先确定服务器所在的时区，例如，当前位置为北京，检查Clock文件参数ZONE为Asia/shanghai，和当前服务器配置为同一时区，如果非当前时区可以做修改。

```
[root@localhost ~]# vi /etc/sysconfig/clock
ZONE="Asia/shanghai"
```

检查当前时间，使用date命令可以看到当前主机时间。

```
[root@localhost ~]# date
Thu Sep 01 10:42:17 CST 2012
```

调整当前主机时间和日期，假设要调整为2012年9月3号，配置完成后，系统就会显示修改好的日期，不过此方式会将时间改为00:00:00。

```
[root@localhost ~]# date -s 20120903
Mon Sep 03 00:00:00 CST 2012
```

调整当前主机时间，假设要调整为11点30分00秒，配置完毕后，系统就会显示修改好的时间，此方式不会影响到日期。

```
[root@localhost ~]# date -s 11:30:00
Mon Sep 03 11:30:00 CST 2012
```

若要修改时间，建议将日期和时间一起调整，假设要调整为2012年09月03日11点30分30秒。

```
[root@localhost ~]# date -s "11:30:30 20120903"
Mon Sep 03 11:30:30 CST 2012
```

系统调整好时间后要同步到BIOS上才算完成，先查看系统时间跟硬件时间是否相同，date为系统时间，hwclock为硬件时间（BIOS），当前两个时间不同步。

```
[root@localhost /]# date ; hwclock -r     //系统时间与 BIOS 时间的对比
Mon Sep 03 11:36:32 CST 2012              //系统时间
Mon 03 Sep 2012 10:57:17 AM CST -0.524230 seconds //硬件时间
```

配置时间时要配置到几乎零误差，就只能跟时间服务器进行同步，时间服务器通常会对国家授时中心公布的站点同步。

```
[root@localhost /]# ntpdate   dns.sjtu.edu.cn //与时间服务器同步
03 Sep 11:00:11 ntpdate[1878]: adjust time server 202.120.2.101 offset -0.012233 sec
```

系统时间同步完成后，再将系统时间写入硬件时间，最后两者再次做比较，时间几乎相同，只有小小的误差。

```
[root@localhost /]# hwclock -w          //将时间写入硬件 BIOS
[root@localhost /]# date ; hwclock -r   //系统时间与 BIOS 时间的对比
Mon Sep 25 03:01:35 CST 2012            //系统时间
Mon 25 Sep 2012 03:01:36 AM CST -0.856179 seconds //硬件时间
```

# 第三部分

# 邮件服务器篇

# 第17章

# Dovecot——接收邮件服务

Dovecot官方网站：http://www.dovecot.org/。

Internet Message Access Protocol（缩写为IMAP，交互式邮件存取协议）是一个应用层协议，它的主要作用是邮件客户端（如Microsoft Outlook、Outlook Express、Foxmail、Mozilla Thunderbird）可以从邮件服务器上获取邮件信息。IMAP和POP3（Protocol Of Post version 3，邮局协议的第三版）是邮件收发最为普遍的Internet标准协议。目前所有的邮件客户端和服务器都对两者予以支持。

## 安装Dovecot服务

### 检查Dovecot服务是否安装

使用前应检查是否已安装Dovecot服务，有的系统会默认安装或安装系统前该服务就已经在安装清单内，若默认为Basic Server则不会安装。

```
[root@localhost ~]# rpm -qa | grep dovecot
dovecot-2.0-0.10.beta6.20100630.el6.x86_64
```

### 安装Dovecot服务

如果操作系统未安装Dovecot软件，建议使用yum在线更新方法进行安装，或者到官网下载Dovecot软件安装。

```
[root@localhost ~]# yum install -y dovecot     //安装 Dovecot 服务

Dependencies Resolved

=======================================================================
```

```
 Package        Arch      Version                         Repository    Size
=======================================================================
Installing:
 dovecot       x86_64   1:2.0-0.10.beta6.20100630.el6      base      2.2 M

Transaction Summary
=======================================================================
Install        1 Package(s)
Upgrade        0 Package(s)

Total download size: 2.2 M
```

## 配置protocols

安装好Dovecot服务后，启动前必须修改配置文件，最重要的就是protocols参数，这个配置会影响Dovecot使用什么协议与客户端通信，主要使用POP3、IMAP协议，默认不启用，开启方式很简单，将配置文件内protocols参数前的#号删除，系统就会自动同时使用IMAP和POP3协议，若要使用其中之一的话，例如不使用POP3，可将POP3、POP3S删除，这样系统就使用IMAP收信。注意CentOS 6和CentOS 5版本系统中Dovecot服务的配置文件路径有所不同。

```
[root@localhost ~]# vi /etc/dovecot/dovecot.conf
# Protocols we want to be serving.
protocols = imap pop3           //将#号删除，配置所要使用的协议
```

> 说明
>
> CentOS 6.x系统Dovecot服务的配置文件路径为/etc/dovecot/dovecot.conf。
>
> CentOS 5.x系统Dovecot服务的配置文件路径为/etc/dovecot.conf。

## 启动Dovecot 服务

修改Dovecot配置后，就可以启动dovecot服务了，为了使邮件服务器提供收信功能，建议将Dovecot服务设为默认启动，以免重新启动系统后忘记启动。

```
[root@localhost ~]# service dovecot start      //Dovecot 启动
Starting Dovecot Imap:                         [  OK  ]
[root@localhost ~]# chkconfig dovecot on       //Dovecot 默认启动
```

Dovecot服务启动若出现失败信息，该失败信息显示端口993已被使用，Dovecot无法正常启动。

```
[root@localhost ~]# service dovecot start
Starting Dovecot Imap: Fatal: listen(993) failed: Address already in use
                                                            [FAILED]
```

主要原因在于端口993正被rpc.statd使用，Dovecot配置文件中protocols配置的imaps的端口也是993，所以必须修改，否则无法启动Dovecot服务。

```
[root@localhost ~]# netstat -tunlp | grep 993
tcp     0   0 0.0.0.0:993            0.0.0.0:*                    LISTEN      2931/rpc.statd
```

## 配置防火墙

所有要对外连接的服务都必须开启防火墙，POP3和IMAP所使用的端口分别为110、143，根据Dovecot配置文件对protocols参数配置的协议开启防火墙。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 110 -j ACCEPT
                                                      //POP3 服务使用端口
-A INPUT -m state --state NEW -m tcp -p tcp --dport 143 -j ACCEPT
                                                      //IMAP 服务使用端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                        [  OK  ]
iptables: Setting chains to policy ACCEPT: filter         [  OK  ]
iptables: Unloading modules:                              [  OK  ]
iptables: Applying firewall rules:                        [  OK  ]
```

## 检查POP3（110）及IMAP（143）是否运行

Dovecot服务基本配置完成后，就可以启动Dovecot服务，使用前建议检查服务是否正常运行，以确保服务可以正常使用。

检查POP3是否运行，若无任何信息代表服务未开启，110为POP3使用的端口。

```
[root@localhost ~]# netstat -tunlp | grep 110
tcp    0    0 0.0.0.0:110 0.0.0.0:*      LISTEN      1795/dovecot
```

```
tcp   0    0 :::110      :::*           LISTEN      1795/dovecot
```

检查IMAP是否运行，若无任何信息代表服务未开启，143为IMAP使用的端口。

```
[root@localhost ~]# netstat -tunlp | grep 143
tcp   0   0 0.0.0.0:143  0.0.0.0:*      LISTEN      1795/dovecot
tcp   0   0 :::143    :::*        LISTEN      1795/dovecot
```

## Dovecot配置允许使用Outlook或Outlook Express接收信件

Dovecot基本配置完成后，除了使用Web方式查看信件之外，Dovecot服务还可以使用邮件客户端接收信件，不过CentOS 6.x系统版本以前不用配置就可以正常收发信件，但是CentOS 6.x系统版本必须要配置才可以正常收发信件，在Dovecot配置文件最后一行添加以下4行信息，这样邮件客户端才可以通过验证接收邮件。

```
[root@mail ~]# vi /etc/dovecot/dovecot.conf
disable_plaintext_auth = no
mail_location = mbox:~/mail:INBOX=/var/mail/%u
pop3_uidl_format = %08Xu%08Xv
pop3_client_workarounds = outlook-no-nuls oe-ns-eoh
```

# 第18章

# Sendmail——发送邮件服务

Sendmail官方网站：http://www.sendmail.org/。

Sendmail 是一套功能强大的邮件传输系统（Mail Transfer Agent），历史也相当悠久，很多Linux操作系统默认都会安装，CentOS 6.x系统以前的版本也是默认安装，不过使用一段时间之后Sendmail 出现了不少重大的安全漏洞，有些漏洞能够入侵服务器，直接影响整个系统的运行，还有Sendmail的配置文件比较麻烦，一般系统管理人员很难轻易掌握，所以有些Linux操作系统不再默认安装。

以下配置皆在CentOS 6.x操作系统上配置，不过建议如果条件允许，可以采用Postfix发送服务器，Sendmail只在这个章节中介绍。

## 18.1 安装配置Sendmail服务

CentOS 6.x版本后已经不默认安装Sendmail服务，CentOS 5.x版本以前还是默认安装，如果要使用Sendmail服务应该先做相关检查及配置。

### 检查Sendmail软件

检查Sendmail软件，若无任何信息表示没有安装Sendmail服务，需自行安装。

```
[root@localhost ~]# rpm -qa | grep sendmail          //检查是否安装 sendmail
sendmail-8.14.4-8.el6.x86_64
```

### 安装Sendmail 服务

安装Sendmail服务的方法有很多种，不过建议使用yum在线更新方法进行安装，除了安装比较方便外，相关的应用软件也会自动安装。使用Sendmail服务需要安装两个基本软件sendmail和sendmail-cf。

```
[root@localhost ~]# yum install -y sendmail sendmail-cf
Dependencies Resolved
========================================================================
 Package     Arch       Version       Repository     Size
========================================================================
Installing:
 Sendmail      x86_64   8.14.4-8.el6      base     717 k
 sendmail-cf  noarch   8.14.4-8.el6      base     184 k
Installing for dependencies:
 Procmail      x86_64   3.22-25.1.el6     base     163 k
Transaction Summary
========================================================================
Install       3 Package(s)
Upgrade       0 Package(s)
Total download size: 1.0 M
```

## 启动Sendmail服务

Sendmail安装完成后，就可以启动Sendmail服务了，建议将Sendmail服务设为默认开机启动，以免重新启动操作系统后忘记启动Sendmail服务，CentOS 6.x以前的版本已配置为默认启动。假如CentOS 6.x要使用Sendmail，记得要将Postfix服务停用，以免两个服务发生冲突。

```
[root@localhost ~]# service sendmail start      //启动 sendmail
Starting sendmail:                              [  OK  ]
Starting sm-client:                             [  OK  ]
[root@localhost ~]# chkconfig sendmail on        //配置 sendmail 默认启用
```

## 配置防火墙

Sendmail默认使用的端口为25，也是SMTP服务默认的端口，需要在防火墙配置中开启SMTP服务端口，若未配置则无法对外发送邮件。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 110 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 143 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
```

```
                                                                //SMTP 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
~
```

防火墙开启SMTP服务端口后，必须重新启动，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                          [  OK  ]
iptables: Setting chains to policy ACCEPT: filter           [  OK  ]
iptables: Unloading modules:                                [  OK  ]
iptables: Applying firewall rules:                          [  OK  ]
```

## 检查Sendmail服务是否运行

检查Sendmail服务是否正常使用SMTP服务端口运行，若未出现任何信息，表示配置有问题，需要重新修改配置文件。

```
[root@localhost ~]# netstat -tunlp | grep sendmail
tcp     0   0 0.0.0.0:25          0.0.0.0:*          LISTEN   1418/sendmail: ace
```

## 配置Sendmail对外连接

编辑Sendmail配置文件，默认为Addr=127.0.0.1，Sendmail服务无法对外连接。

```
[root@localhost ~]# vi /etc/mail/sendmail.cf
# SMTP daemon options
O DaemonPortOptions=Port=smtp,Addr=127.0.0.1, Name=MTA
                                                //默认 127.0.0.1 无法对外连接
# SMTP client options
#O ClientPortOptions=Family=inet, Address=0.0.0.0
```

测试Sendmail服务是否可以对外连接，使用客户端telnet方法测试邮件服务器，结果发现Sendmail服务无法对外连接。

```
C:\Users\jerry>telnet 192.168.233.222 25
正连接到 192.168.233.222...无法开启到主机的连接，在端口 25: 连接失败
```

要将Sendmail对外连接，必须将Addr=127.0.0.1改成0.0.0.0。

```
[root@localhost ~]# vi /etc/mail/sendmail.cf
# SMTP daemon options
O DaemonPortOptions=Port=smtp,Addr=0.0.0.0, Name=MTA //0.0.0.0 允许对外连接
```

**说明**

不可以配置邮件主机IP地址，以免内部用户收不到信件。

修改完毕后，必须重新启动Sendmail服务，配置文件才会生效，第一次重新启动会出现Shutting down sendmail Fail的错误信息，不过再重新启动一次就不会出现此信息了。

```
[root@localhost ~]# service sendmail restart
Shutting down sm-client:                                    [  OK  ]
Shutting down sendmail:                                     [  OK  ]
Starting sendmail:                                          [  OK  ]
Starting sm-client:                                         [  OK  ]
```

重新启动Sendmail服务后，再次测试，主机使用telnet 邮件服务器的IP地址，出现Sendmail名称表示成功。

```
[root@localhost ~]# telnet 192.168.233.222 25
Trying 192.168.233.222...
Connected to 192.168.233.222.
Escape character is '^]'.
220 localhost.localdomain ESMTP Sendmail 8.14.4/8.14.4; Sun, 4 Sep 2012 23:40:39 -0400
```

客户端telnet sendmail主机IP地址，也显示连接成功的消息。

```
220 localhost.localdomain ESMTP Sendmail 8.14.4/8.14.4; Sun, 4 Sep 2012 23:40:15
 -0400
```

### 配置对外发信

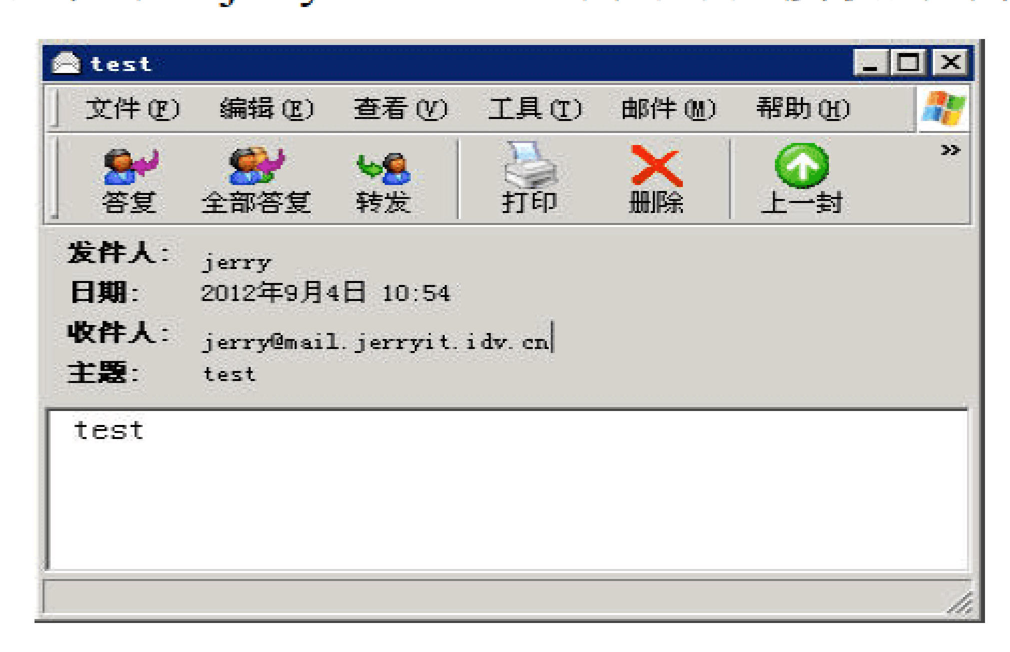
配置好Sendmail的对外连接后，需要配置邮件服务器权限，这样才可以使用此邮件服务器正确地对外发信，否则会发生Relaying denied。

```
[root@mail ~]# vi /etc/mail/access
# Check the /usr/share/doc/sendmail/README.cf file for a description
# of the format of this file. (search for access_db in that file)
# The /usr/share/doc/sendmail/README.cf is part of the sendmail-doc
# package.
#
# If you want to use AuthInfo with "M:PLAIN LOGIN", make sure to have the
# cyrus-sasl-plain package installed.
#
# By default we allow relaying from localhost...
Connect:localhost.localdomain           RELAY
Connect:localhost                       RELAY
Connect:127.0.0.1                       RELAY
Connect:jerryit.idv.cn                  RELAY //配置域名
Connect:192.168.233.*                   RELAY //配置主机对外 IP 地址或网段
```

## 18.2 配置邮件地址名称

创建好邮件服务器后，外面的用户要发送邮件给邮件主机内的用户，在@后面就会加上完

整的邮件主机名，例如，给DNS配置MX记录为mail主机，域名为jerryit.idv.cn，示例用户是jerry，外部用户发送邮件到这台邮件服务器时，收件者就必须输入【jerry@mail.jerryit.idv.cn】，如下图所示，mail是邮件主机的主机名，一般不需要显示，通常会输入【jerry@jerryit.idv.cn】，不过用户无法收到信，原因在于【jerryit.idv.cn】不是可以接收的邮件地址名称。




要配置可接收的邮件地址名称为【jerryit.idv.cn】，必须修改配置文件，添加邮件地址名称。

```
[root@localhost ~]# vi /etc/mail/local-host-names
# local-host-names - include all aliases for your machine here.
jerryit.idv.cn          //接收邮件地址名称
```

使用上述方法配置完后，@后面加上【mail.jerryit.idv.cn】就无法再收到信了，假如再发送邮件就会出现如下的错误信息。不过配置文件内可添加多个接收邮件的地址，建议保留两个邮件地址名称，【mail.jerryit.idv.cn】及【jerryit.idv.cn】。

```
The original message was received at Tue, 4 Sep 2012 19:47:26 +0800
from [192.168.233.222]

   ----- The following addresses had permanent fatal errors -----
<jerry@jerryit.idv.cn>
    (reason: 553 5.3.5 system config error)

   ----- Transcript of session follows -----
553 5.3.5 jerryit.idv.cn. config error: mail loops back to me (MX problem?)
554 5.3.5 Local configuration error
```

**说明**

在CentOS 6.0之后如果只配置了【jerryit.idv.cn】邮件地址名称，不会发送错误信息，两封邮件都能收到。

修改完配置文件后，必须重新启动Sendmail服务，配置才会生效。

```
[root@mail ~]# service sendmail restart
Shutting down sm-client:                                   [  OK  ]
Shutting down sendmail:                                    [  OK  ]
Starting sendmail:                                         [  OK  ]
Starting sm-client:                                        [  OK  ]
```

再次发送邮件时，邮件地址输入【jerry@jerryit.idv.cn】，这样就可以正常接收到邮件了，如下图所示。




## 18.3 配置邮件发送和接收附件的大小

接收容量过大的邮件会导致邮件主机运行变慢，造成用户信箱马上爆满，甚至导致带宽被占据，若遭到邮件容量过大的恶意攻击时，还会导致网络瘫痪，这样就需要限制邮件发送或接收的大小，以避免故意发送大容量邮件的情况出现，所以要有效地管理信件容量大小。Sendmail服务可以配置每封信件发送或接收的大小。

### 修改Sendmail配置文件

编辑Sendmail配置文件，将MaxMessageSize参数前的#号删除，并限制配置容量大小，如限制为2MB。

```
[root@mail ~]# vi /etc/mail/sendmail.cf
# maximum message size
O MaxMessageSize=2048000                                //默认未限制容量
```

修改配置后，必须重新启动Sendmail服务，这样配置才会生效。

```
[root@mail ~]# service sendmail restart
Shutting down sm-client:                              [  OK  ]
Shutting down sendmail:                               [  OK  ]
Starting sendmail:                                    [  OK  ]
Starting sm-client:                                   [  OK  ]
```

### 测试信件容量

写一封邮件来测试发送情况，如果出现下图所示的信息，是告知你的邮件容量超过2MB而无法发送，这样就表示对每封信件容量大小的限制成功。



OpenWebMail信息警告邮件容量超过2MB，所以无法发送邮件。



## 18.4 配置邮件账号别名

邮件账号的别名一般在电子邮件不想对外公布或者是此账号为公用账号的情况下使用，当用户离职或变更职务后，可将该别名指定到新的用户账号，此后当众多发件人发送给该电子邮件账号时，信件会转给新的用户账号，这样可以省去不少通知的时间。下面介绍几种别名的应用方法，可根据实际情况进行配置。

### 单一邮件账号，单一账户别名

此方法只有一个别名对应一个账号。

| 示例介绍 | |
|---|---|
| 账户别名 | 账号 |
| jerryit | jerry |

编辑/etc/aliases配置文件，输入方法可以参考配置文件内的示例。

```
 [root@localhost ~]# vi /etc/aliases
…中间省略…
info:           postmaster
marketing:      postmaster
sales:          postmaster
support:        postmaster
jerryit:        jerry                        //配置 jerry 账户别名为 jerryit
# trap decode to catch security attacks
```

```
decode:         root
# Person who should get root's mail
#root:          marc
```

> **说明**
>
> 账户别名后面有一个【:】符号。

将电子邮件账户别名输入完后，必须让别名生效，这样账户别名才会生效，若有错误表示输入有错，可按错误信息提示解决。

```
[root@localhost ~]# newaliases
/etc/aliases: 77 aliases, longest 10 bytes, 777 bytes total
```

若配置好账户别名后，没有让账户别名生效，则无法发送邮件，错误信息为【550 User unknown】，如下图所示。




使用其他邮件账号发送邮件测试，收件人输入【jerryit@jerryit.idv.cn】，输入完毕后，按【发送】。

查看jerry账号的信箱，可以看到一封发送给jerryit@jerryit.idv.cn的信件，如下图所示，表示成功。

## 单一邮件账号，多个账号别名

此方法是多个别名指定一个账号，这里配置了三个别名指定给账号jerry使用。

| 账户别名 | 账号 |
|---|---|
| jerryit | jerry |
| jerry0822 | jerry |
| jerry710822 | jerry |

编辑/etc/aliases，依次输入，一个输入错误则无法使用。

```
[root@localhost ~]# vi /etc/aliases
…中间省略…
jerryit:        jerry               //依次输入三个别名
jerry0822:      jerry
jerry710822:    jerry
```

输入完账户别名后，必须让别名生效，依次寄信给这三个账户别名，若三封信都收到表示配置成功。

```
[root@localhost ~]# newaliases
/etc/aliases: 79 aliases, longest 10 bytes, 807 bytes total
```

## 单一账号别名，多个账号

此方法适用于群组发送信件，比如要给业务部门发送一封信，将部门所有账号加入同一别名，则收件者收到信件后，只会看到是发送给该部门的信。

| 账户别名 | 账号 |
|---|---|
| jerryit | jerry,mary,Ken |

依次输入要加入该别名的电子邮件账号。

```
[root@localhost ~]# vi /etc/aliases
…中间省略…
sales:          postmaster
support:        postmaster
jerryit:        jerry,mary,ken          //一个别名三个账号
```

输入完账户别名后，必须让别名生效，发送邮件给账户别名jerryit测试，查看三个账号会不会都收到信。

```
[root@localhost ~]# newaliases
/etc/aliases: 77 aliases, longest 14 bytes, 786 bytes total
```

## 别名账号的账号清单文件

此情形用于过多账号或有非当前邮件主机的账号。

| 别名 | 账号清单文件名 |
|---|---|
| jerryit | Mailaddr.list |

示例中在根目录创建别名账号列表，名称为mailaddr.list，输入所要发送的账号，也可以输入非当前邮件主机的邮件地址，输入完成后保存退出。

```
[root@localhost ~]# vi /mailaddr.list
jerry,ken,jerry710822@gmail.com         //账号清单
```

编辑/etc/aliases，内容以include载入。

```
[root@localhost ~]# vi /etc/aliases
info:           postmaster
marketing:      postmaster
sales:          postmaster
support:        postmaster
jerryit:        ":include:/mailaddr.list"        //配置清单别名
```

账户别名输入完后，必须让别名生效。发送一封信给账户别名jerryit，测试外部信箱可不可以收到。

```
[root@localhost ~]# newaliases
/etc/aliases: 77 aliases, longest 25 bytes, 797 bytes total
```

## 配置别名时出现 duplicate alias name错误信息

若使别名生效时，出现duplicate alias name错误信息，这样别名就无法生效。

```
[root@localhost ~]# newaliases
/etc/aliases: line 90: sales... Warning: duplicate alias name sales
/etc/aliases: 77 aliases, longest 25 bytes, 795 bytes total
```

其实问题很简单，就是在/etc/aliases配置文件里，别名名称可能重复，例如，/etc/aliases里有个别名叫做sales，如果再输入相同的别名，就会发生错误。

```
[root@localhost ~]# vi /etc/aliases
info:           postmaster
marketing:      postmaster
sales:          postmaster              //有两个 sales 别名
support:        postmaster
sales:          ":include:/mailaddr.list"
```

# 18.5 配置Sendmail账号认证

账号认证就是在邮件主机中加入身份验证的机制。以SMTP来说，原来的设计并没有身份验证的部分，只要符合Mail Server中的relay配置，就可以通过Mail Server发送。当使用者不在relay配置范围内的时候，只要你的username和password通过验证，Mail Server就允许发送邮件。

## 安装 SASL 认证软件

账号认证功能需要安装cyrus-sasl软件，若没有安装，请使用yum在线更新方法安装。

```
[root@localhost ~]# rpm -qa |grep cyrus-sasl
cyrus-sasl-devel-2.1.23-8.el6.x86_64
cyrus-sasl-lib-2.1.23-8.el6.x86_64
cyrus-sasl-gssapi-2.1.23-8.el6.x86_64
cyrus-sasl-plain-2.1.23-8.el6.x86_64
cyrus-sasl-ldap-2.1.23-8.el6.x86_64
cyrus-sasl-ntlm-2.1.23-8.el6.x86_64
cyrus-sasl-sql-2.1.23-8.el6.x86_64
cyrus-sasl-md5-2.1.23-8.el6.x86_64
cyrus-sasl-2.1.23-8.el6.x86_64
```

## 修改sendmail.mc配置文件

修改sendmail.mc配置文件后，删除前面的dn1，就可以生成新的sendmail.cf文件。

```
[root@localhost ~]# vi /etc/mail/sendmail.mc
dnl # PLAIN is the preferred plaintext authentication method and used by
dnl # Mozilla Mail and Evolution, though Outlook Express and other MUAs do
dnl # use LOGIN. Other mechanisms should be used if the connection is not
dnl # guaranteed secure.
dnl # Please remember that saslauthd needs to be running for AUTH.
dnl #
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
```

DAEMON_OPTIONS的Addr=127.0.0.1，必须修改为0.0.0.0。

```
[root@localhost ~]# vi /etc/mail/sendmail.mc
dnl # The following causes sendmail to only listen on the IPv4 loopback address
dnl # 127.0.0.1 and not on any other network devices. Remove the loopback
dnl # address restriction to accept email from the internet or intranet.
dnl #
DAEMON_OPTIONS(`Port=smtp,Addr=0.0.0.0, Name=MTA')dnl
```

## 生成sendmail.cf配置文件

将sendmail.mc复制至/usr/share/sendmail-cf/cf目录下，可能会发现没有/usr/share/sendmail-cf/cf目录。

```
[root@localhost ~]# cp /etc/mail/sendmail.mc /usr/share/sendmail-cf/cf
cp: cannot create regular file `/usr/share/sendmail-cf/cf': No such file or directory
```

若没有/usr/share/sendmail-cf/cf目录，表示没有安装sendmail-cf，可使用yum在线更新方法

进行安装。

```
[root@localhost ~]# yum install sendmail-cf
Dependencies Resolved
======================================================================
 Package        Arch          Version            Repository       Size
======================================================================
Installing:
 sendmail-cf  i386          8.13.8-8.1.el5_7     updates          306 k
Updating for dependencies:
 sendmail     i386          8.13.8-8.1.el5_7     updates          624 k
Transaction Summary
======================================================================
Install       1 Package(s)
Upgrade       1 Package(s)
Total download size: 929 k
```

安装完sendmail-cf软件后，再次生成新的sendmail-cf配置文件，复制sendmail.mc配置文件至/usr/share/sendmail-cf/cf目录下。

```
[root@localhost ~]# cp /etc/mail/sendmail.mc /usr/share/sendmail-cf/cf
```

复制好配置文件后，进入sendmail-cf的cf目录，使用scripts生成新的sendmail.cf配置文件。

```
[root@localhost ~]# cd /usr/share/sendmail-cf/cf
[root@localhost cf]# sh Build sendmail.cf     //生成新的 sendmail.cf
Using M4=/usr/bin/m4
rm -f sendmail.cf
/usr/bin/m4 ../m4/cf.m4 sendmail.mc > sendmail.cf || ( rm -f sendmail.cf && exit 1 )
echo "### sendmail.mc ###" >>sendmail.cf
sed -e 's/^/# /' sendmail.mc >>sendmail.cf
chmod 444 sendmail.cf
```

在使用新的配置文件前先将旧的sendmail.cf文件备份，将/usr/share/sendmail-cf/cf文件目录下的sendmail.cf文件复制到/etc/mail/目录。

```
[root@localhost cf]# mv /etc/mail/sendmail.cf /etc/mail/sendmail.cf.old
                                     //备份 sendmail.cf
[root@localhost cf]# cp sendmail.cf /etc/mail/sendmail.cf
                                     //复制新的 sendmail.cf
```

## 重新启动SASL及Sendmail 服务

所有配置完成后，重新启动Sendmail及SASL服务，并将SASL设为默认启动。

```
[root@localhost cf]# service saslauthd start
Starting saslauthd:                                    [  OK  ]
[root@localhost cf]# chkconfig saslauthd on
[root@localhost cf]# service sendmail restart
```

```
Shutting down sm-client:                                  [  OK  ]
Shutting down sendmail:                                   [  OK  ]
Starting sendmail:                                        [  OK  ]
Starting sm-client:                                       [  OK  ]
```

## 验证SASL是否有误

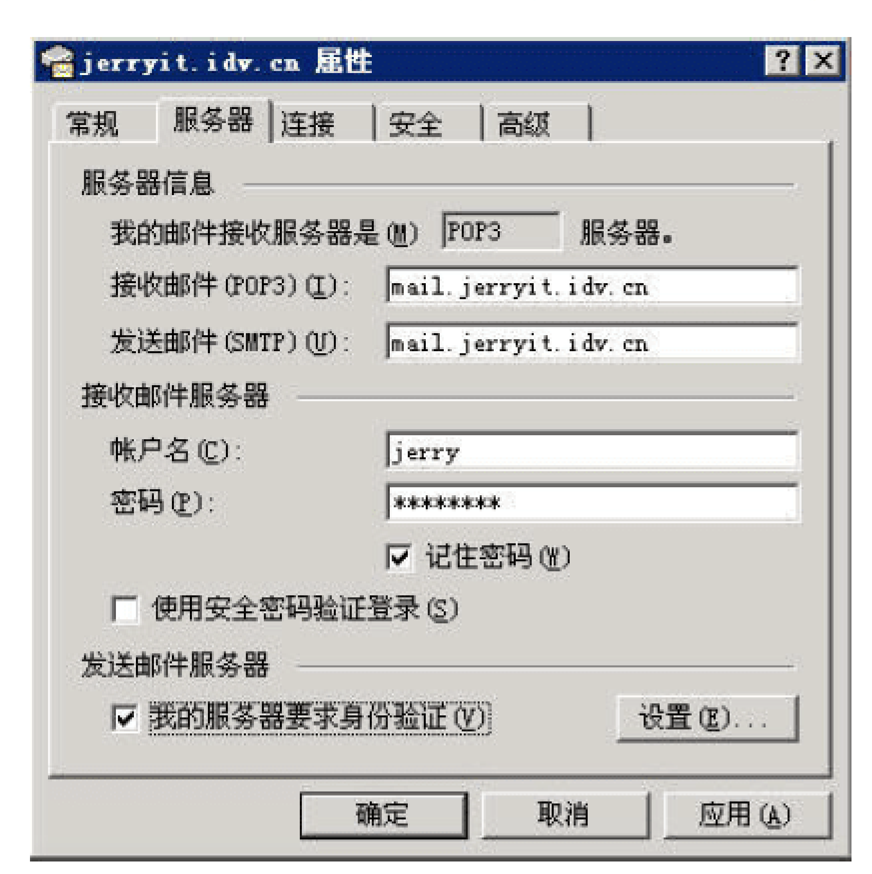
使用telnet方法检查，出现AUTH LOGIN PLAIN表示验证成功。

```
[root@localhost cf]# telnet  localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1) .
Escape character is '^]'.
220 localhost.localdomain ESMTP Sendmail 8.13.8/8.13.8; Tue, 02 Sep 2012 19:22:52 -0400
ehlo localhost
250-localhost.localdomain Hello localhost.localdomain [127.0.0.1], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH LOGIN PLAIN           //Sendmail 有验证功能
250-DELIVERBY
250 HELP
```

## 测试客户端是否可以验证

在客户端测试将邮件发送到外面的信箱，如果没有选择【我的服务器要求身份验证】，就会发生错误，表示配置成功，注意不可以发送到内部信箱，否则不会起到身份验证功能。

选择【工具】→【账户】→【邮件】，单击所要认证的账号，然后输入账号信息，在【服务器】选项中，在【发送邮件服务器】下勾选【我的服务器需要验证】。



若未勾选【我的服务器需要验证】，则该账号使用Outlook软件发送邮件时会出现服务器拒绝信息，无法寄出邮件。



# 第 19 章

# Postfix——发送邮件服务

Postfix官方网站：http://www.postfix.org/。

Postfix 服务是一个快速、易于管理、安全性高的邮件发送程序，而且能很好地兼容Sendmail服务，主要是为了让原有的使用者操作方便，因此Postfix服务的外部运行和 Sendmail服务运行一样，但实际上内部是完全不同的设计。

## 19.1 安装 Postfix服务

下面介绍如何配置简易的Postfix服务器，其安装非常简单，经过一些基本配置，就可以让邮件服务器正常发送邮件。

### 安装Postfix 服务

安装Postfix服务前，应检查Postfix服务是否安装，其实从CentOS 6.x操作系统之后，系统就会默认安装及启动，但是以前默认安装的Sendmail服务，现在则必须要自行安装，下面的操作是为了检查Postfix软件。

```
[root@localhost ~]# rpm -qa | grep postfix
postfix-2.6.6-2.1.el6_0.x86_64
```

假设没有安装Postfix服务软件，或是想要更新到最新的Postfix服务软件，毕竟CentOS光盘内的软件不一定是最新版本，可以使用yum在线更新方式进行安装，既方便又快速。

```
[root@localhost ~]# yum install -y  postfix
Dependencies Resolved
========================================================================
 Package       Arch        Version            Repository            Size
========================================================================
Installing:
 postfix     x86_64    2:2.6.6-2.1.el6_0       updates             2.0 M
Transaction Summary
========================================================================
```

```
Install        1 Package(s)
Upgrade        0 Package(s)
Total download size: 2.0 M
```

## 配置基本Postfix服务

CentOS 6.x系统安装好Postfix服务后，需要做几项配置，才可以正常收发信件，以下几个配置是在安装好后必要进行的，尤其是mydestination和inet_interfaces参数，若不配置就无法收发信件。

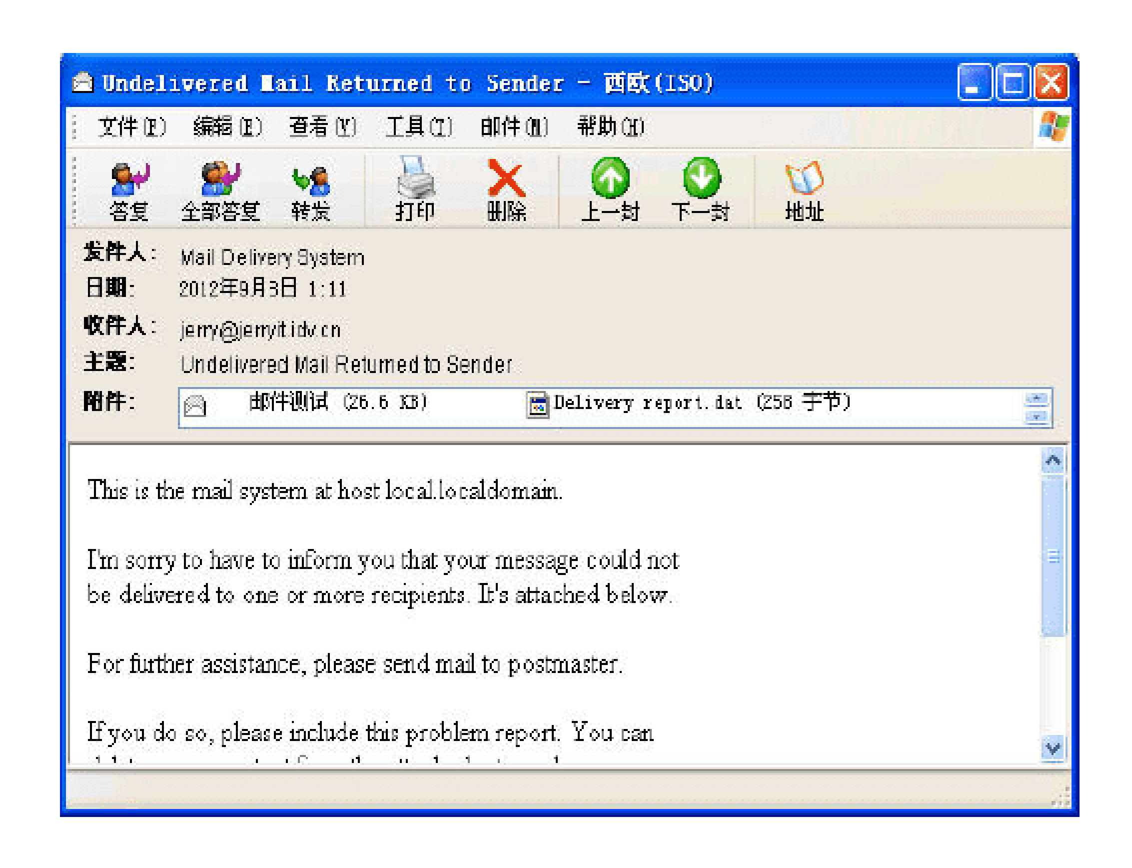
- **myhostname:** 这个参数顾名思义就是要配置计算机名称，不过这里需要输入的是FQDN完整名称，而不只是计算机名称，所谓的FQDN就是计算机名称加上全称域名。

```
[root@localhost ~]# vi /etc/postfix/main.cf
# The myhostname parameter specifies the internet hostname of this
# mail system. The default is to use the fully-qualified domain name
# from gethostname(). $myhostname is used as a default value for many
# other configuration parameters.
#
#myhostname = host.domain.tld
#myhostname = virtual.domain.tld
myhostname = mail.jerryit.idv.cn                          //配置完整的 FQDN
```

- **mydestination:** 这个参数是可以接受收发信件的域名，在该行最后面添加收发邮件的域名，记得每个域名之间需要加上【,】分隔，这样才可以正常收发信件。

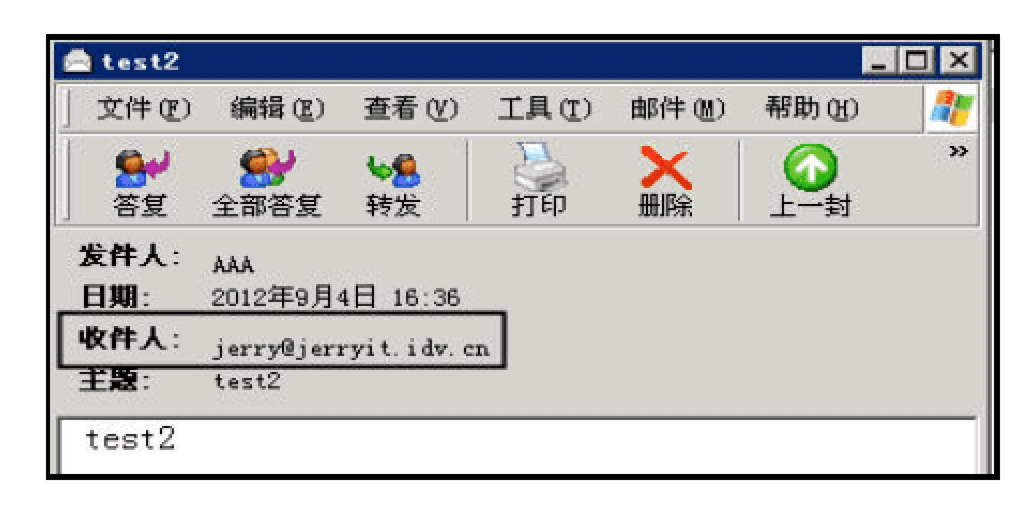
```
[root@localhost ~]# vi /etc/postfix/main.cf
#
mydestination = $myhostname, localhost.$mydomain, localhost, jerryit.idv.cn
#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain,
```

Mydestination参数若没有配置，则会无法发送信件到Internet上的邮件服务器，就算信件勉强发送，一分钟以内就会收到一封主题为Undelivered Mail Returned to Sender的退信，无法将信件寄出。



Mydestination参数还有另一个功能，若没有配置，先不考虑是不是可以对外开放，假如发件人使用Outlook之类的软件给收件者发送信件，收件者@后面的后缀就必须是完整的FQDN，意思就是说发送邮件给收件者时需要在@后输入完整的FQDN，收件者才可以收到信。

以上介绍可能不是很清楚，下面举例来说明。计算机名称为mail，域名为jerryit.idv.cn，mydestination没有配置，在发送邮件时，@后缀则必须输入mail.jerryit.idv.cn，在mydestination配置中加上jerryit.idv.cn，再次发送邮件时，@后的后缀只要输入jerryit.idv.cn即可，而非mail.jerryit.idv.cn，不过经过上述配置后，发送邮件时，@后的后缀若输入mail.jerryit.idv.cn，收件者就无法收到信件，所以为了避免收不到信，建议在mydestination参数后添加这两个域名。




- **inet_interfaces:** 默认配置为localhost，所以只会处理本机网络界面接收的信息。若要处理所有网络界面，必须将inet_interfaces由默认的localhost改成all。

```
[root@localhost ~]# vi /etc/postfix/main.cf
# The inet_interfaces parameter specifies the network interface
# addresses that this mail system receives mail on.  By default,
# the software claims all active interfaces on the machine. The
# parameter also controls delivery of mail to user@[ip.address].
#
# See also the proxy_interfaces parameter, for network addresses that
# are forwarded to us via a proxy or network address translator.
#
# Note: you need to stop/start Postfix when this parameter changes.
#
#inet_interfaces = all
#inet_interfaces = $myhostname
#inet_interfaces = $myhostname, localhost
inet_interfaces = all                        //默认为 localhost，修改为 all
```

> **说明**
>
> 这里不可以配置MAIL主机IP地址，以免内部收不到信件。

- **inet_protocols:** 参数默认为all，所以可以同时支持IPv4和IPv6协议。

```
[root@localhost ~]# vi /etc/postfix/main.cf
# Enable IPv4, and IPv6 if supported
inet_protocols = all         //默认为 all，可以修改为 ipv4 或 ipv6，配置值要小写
```

Postfix服务使用25端口，除了IPv4协议的0.0.0.0外，还会有IPv6协议的:::。若不想使用IPv6

协议，可以将配置值由all修改成ipv4，此配置可根据自己需要进行修改，重要性并不大。

```
[root@localhost ~]# netstat -tunlp | grep 25
tcp      0   0 0.0.0.0:25              0.0.0.0:*          LISTEN      3297/master
tcp      0   0 :::25                    :::*              LISTEN      3297/master
```

## 配置防火墙

Postfix服务默认使用的端口就是SMTP的端口25，在防火墙配置文件中开放25端口，允许Postfix服务开放对外连接。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
                                                          //Postfix 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

修改防火墙后，必须要重新启动防火墙服务，配置才生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

## 启动Postfix服务

确定Postfix服务及防火墙配置完成后，接下来就是重新启动Postfix服务，并将Postfix服务设为默认开机启动，CentOS 6.x默认已经配置为启动。

```
[root@localhost ~]# service postfix restart
Shutting down postfix:                                     [  OK  ]
Starting postfix:                                          [  OK  ]
[root@localhost ~]# chkconfig postfix on
```

Postfix服务启动后，测试Postfix服务是否可以对外连接，不可以测试IP地址127.0.0.1，要

测试对外连接的IP地址，信息中显示Postfix代表可以正常对外连接。

```
[root@localhost ~]# telnet 192.168.233.192 25
Trying 192.168.233.192...
Connected to 192.168.233.192.
Escape character is '^]'.
calhost.localdomain ESMTP Postfix        //代表正常对外连接
```

说明

192.168.233.192为Postfix主机IP地址，根据需求环境的不同而不同。

# 19.2 配置信箱容量

信箱容量是给予用户可以存放信件的空间，因为服务器硬盘容量不是无限大，就算硬盘容量很大，但是当每个信箱容量都很大时，服务器性能也不会很好，所以有效地限制服务器用户信箱容量，才最重要。

## 配置信箱容量上限

Postfix服务默认信箱容量为50MB，若不做任何配置，当用户信箱容量到达50MB后，就会无法收到信件，所以就需要配置信箱容量上限，下面介绍如何修改信箱容量上限及配置无容量限制。

例如，限制信箱容量为10MB，编辑Postfix配置文件，默认没有mailbox_size_limit这个配置参数，需要自行在最后一行添加。

```
[root@localhost ~]# vi /etc/postfix/main.cf
…中间省略…
mailbox_size_limit = 10240000      //限制信箱容量为 10MB，默认为 50MB
```

如果想要信箱容量上限不受限，将mailbox_size_limit参数配置为0，则信箱容量就不会再受到默认50MB的限制。

```
[root@localhost ~]# vi /etc/postfix/main.cf
…中间省略…
mailbox_size_limit = 0       //0 为无上限
```

以上两种示例配置完毕，且Postfix配置文件修改后，必须要重新启动Postfix服务，配置才会生效。

```
[root@localhost ~]# service postfix restart
Shutting down postfix:                                     [  OK  ]
Starting postfix:                                          [  OK  ]
```

## 测试信箱容量上限及无上限

当信箱容量到达约10MB时，看看是否可以再发送邮件给该收件者，测试结果如果不能发送，说明配置限制10MB容量成功。

| 默认邮件夹 | 新邮件 | 邮件 | 大小 |
|---|---|---|---|
| 收件箱 | 25 | 25 | 9.5MB |
| 存档箱 | 0 | 0 | 0 |
| 已发送邮件 | 0 | 0 | 0 |
| 草稿箱 | 0 | 0 | 0 |
| 废件箱 | 0 | 0 | 0 |
| 垃圾邮件箱 | 0 | 0 | 0 |
| 病毒邮件箱 | 0 | 0 | 0 |
| 总计 | 25 | 25 | 9.5MB |

当信箱容量超过50MB，看看是否可以继续发送邮件给该收件者，测试结果如果能超过50MB，代表信箱容量可以超过默认的50MB，也可以到达无上限，如果实体硬盘空间已满，也无法收到邮件。

| 默认邮件夹 | 新邮件 | 邮件 | 大小 |
|---|---|---|---|
| 收件箱 | 32 | 32 | 50.1MB |
| 存档箱 | 0 | 0 | 0 |
| 已发送邮件 | 0 | 0 | 0 |
| 草稿箱 | 0 | 0 | 0 |
| 废件箱 | 0 | 0 | 0 |
| 垃圾邮件箱 | 0 | 0 | 0 |
| 病毒邮件箱 | 0 | 0 | 0 |
| 总计 | 32 | 32 | 50.1MB |

# 19.3 单封信件容量

现行的邮件服务器不管发送或接收邮件，通常都会限制单封信件的容量大小，最常见的Exchange Server就配置了单封信件容量，配置发送或接收的信件容量大小可以避免接收容量过大的邮件，避免导致邮件服务器运行性能不佳，连带使局域网带宽受到影响，所以有效地限制单封信件容量大小是很必要的。

## 配置单封信件容量上限

Postfix服务可以配置每封信件发送或接收的大小，需要编辑Postfix配置文件，默认没有配置message_size_limit参数，必须在最后一行添加，例如，限制每封信件的大小为2MB，单封信件容量可根据使用情况而定。

```
[root@localhost ~]# vi /etc/postfix/main.cf
```

```
…中间省略…
message_size_limit = 2048000          //信件容量上限
```

修改Postfix配置文件后，必须要重新启动Postfix服务，配置才会生效。

```
[root@localhost ~]# service postfix restart
Shutting down postfix:                                     [  OK  ]
Starting postfix:                                          [  OK  ]
```

## 测试单封信件容量上限

使用OpenWebMail客户端写一封新邮件测试，信息会提示邮件容量过大无法发送，这样就代表限制单封信件容量成功。




# 19.4 配置邮件账号身份验证

以SMTP来说，原来的设计并没有所谓身份验证的部分，只要符合Mail Server中的relay配置，就可以通过Mail Server送信。在邮件服务器中加入身份验证的机制，当使用者不在relay配置范围内的时候，只要用户名和用户密码通过验证，Mail Server就可以发送邮件。

## 安装SASL认证软件

要使用账号认证就必须要安装SASL认证软件，否则无法使用身份验证功能，配置前先检查是否安装，CentOS6.x版本默认自动安装。

```
[root@localhost ~]# rpm -qa | grep cyrus-sasl
cyrus-sasl-lib-2.1.23-8.el6.x86_64
cyrus-sasl-gssapi-2.1.23-8.el6.x86_64
cyrus-sasl-plain-2.1.23-8.el6.x86_64
cyrus-sasl-2.1.23-8.el6.x86_64
```

## 配置Postfix身份验证

安装SASL认证软件后，需要编辑Postfix配置文件才可以达到身份验证功能，需要将以下

配置信息添加到Postfix配置文件的最后一行。

```
[root@localhost ~]# vi /etc/postfix/main.cf
…中间省略…
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions =
permit_mynetworks,permit_sasl_authenticated,reject_unauth_destination
```

## 启动SASL服务

Postfix配置完毕后，SASL服务就可以启动了，此服务与Postfix服务是搭配使用的，所以也必须要配置成默认启动。

```
[root@localhost ~]# service saslauthd start
Starting saslauthd:                                        [  OK  ]
[root@localhost ~]# chkconfig saslauthd on
```

## 重新启动Postfix服务

SASL服务启动完毕后，由于修改了Postfix配置文件，所以必须要重新启动Postfix服务，这样配置才会生效。

```
[root@localhost ~]# service postfix restart
Shutting down postfix:                                     [  OK  ]
Starting postfix:                                          [  OK  ]
```

## 验证Postfix + SASL服务

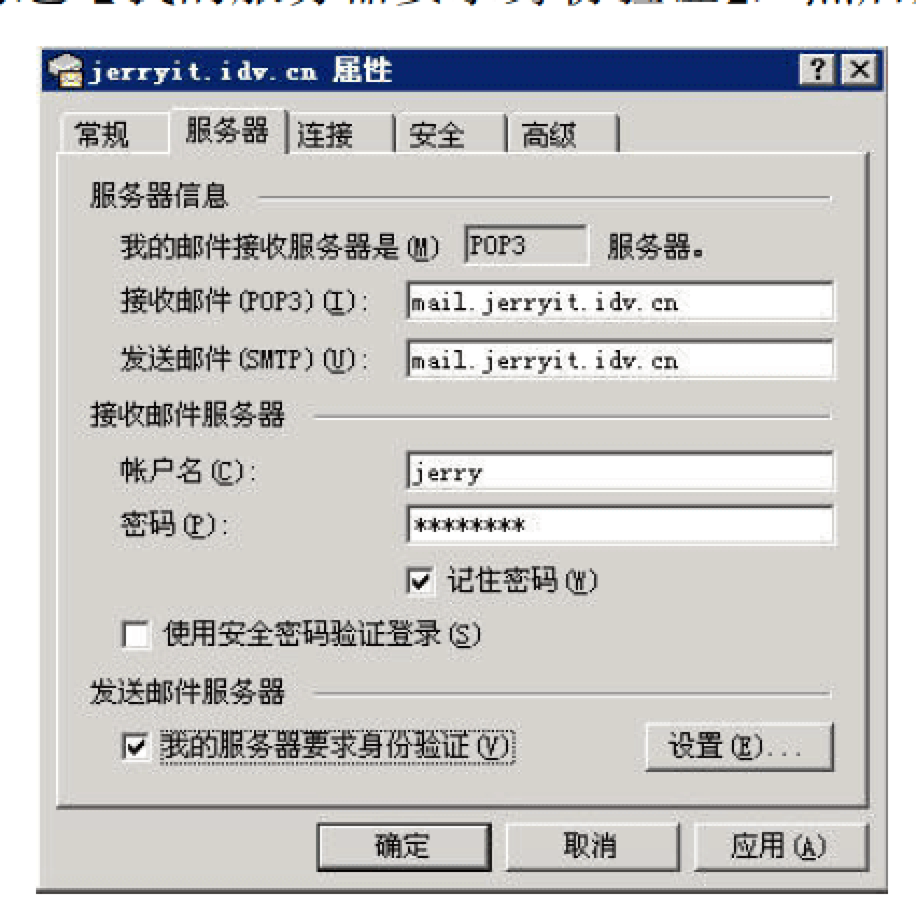
启动Postfix和SASL服务之后，必须要验证配置是否正常，可使用telnet方法进行验证。

```
[root@localhost ~]# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 localhost.localdomain ESMTP Postfix
ehlo localhost                    //验证是否正常
250-localhost.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN LOGIN              //出现此两行代表验证成功
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
```

```
250-8BITMIME
250 DSN
```

## 测试客户端是否可以验证

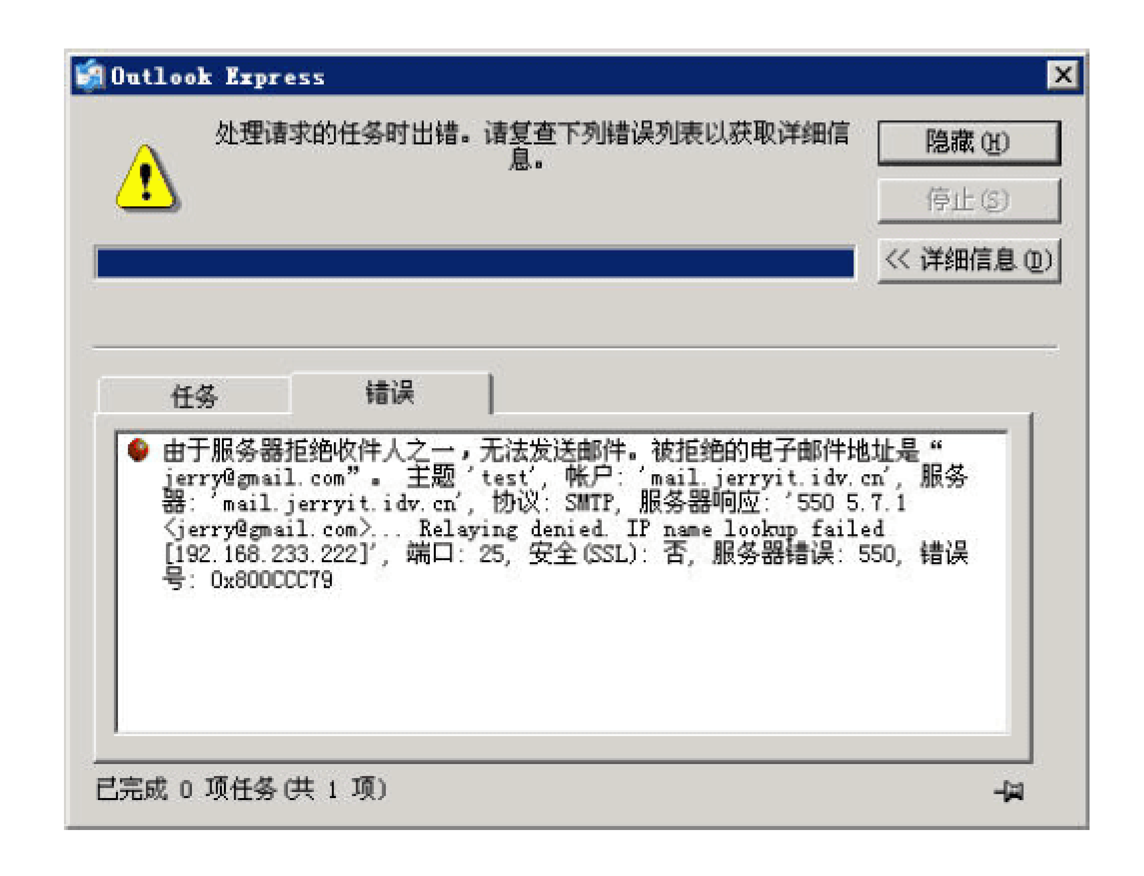
Postfix和SASL服务正确启动验证后，接下来就是配置客户端，选择【工具】→【账户】→【邮件】，单击选择所要认证的账号，然后按下属性，在该账号属性的【服务器】选项中，在【发送邮件服务器】下勾选【我的服务器要求身份验证】，然后发送一封信测试。




检查邮件日志文件，若勾选了【我的服务器要求身份验证】，在日志文件内可以看到sasl_method=LOGIN及sasl_username信息。

```
[root@localhost ~]# cat /var/log/maillog
Aug 13 09:52:16 localhost postfix/smtpd[5177]: connect from unknown[192.168.233.150]
Aug 13 09:52:16 localhost postfix/smtpd[5177]: B0E5BA1AEC:
client=unknown[192.168.233.150], sasl_method=LOGIN, sasl_username=jerry
Aug 13 09:52:16 localhost postfix/cleanup[5181]: B0E5BA1AEC:
message-id=<CB70B67D2E544739A87B9643B5515558@adminf4d1e38c8>
Aug 13 09:52:16 localhost postfix/qmgr[5085]: B0E5BA1AEC: from=<jerry@jerryit.idv.cn>,
size=667, nrcpt=1 (queue active)
Aug 13 09:52:16 localhost postfix/smtpd[5177]: disconnect from unknown[192.168.233.150]
Aug 13 09:52:18 localhost dovecot: pop3-login: Login: user=<jerry>, method=PLAIN,
rip=192.168.233.150, lip=192.168.233.192, mpid=5187
Aug 13 09:52:18 localhost dovecot: pop3(jerry): Disconnected: Logged out top=0/0, retr=0/0,
del=0/0, size=0
Aug 13 09:52:19 localhost postfix/smtp[5182]: B0E5BA1AEC: to=<jerry@gmail.com>,
relay=gmail-smtp-in.l.google.com[74.125.91.26]:25, delay=2.8, delays=0.11/0.03/1.1/1.6,
dsn=2.0.0, status=sent (250 2.0.0 OK 1318441948 h7si815275qct.156)
Aug 13 09:52:19 localhost postfix/qmgr[5085]: B0E5BA1AEC: removed
```

如果未勾选【我的服务器要求身份验证】，则该账号使用Outlook之类的软件发送邮件时，可能会出现服务器拒绝信息，无法发送邮件。




## 19.5 Sendmail和Postfix的切换

邮件服务器发信的MTA有Sendmail和Postfix两种，Sendmail算是历史久远的一款，很多Linux默认就会启用，Postfix为后起之秀，比Sendmail更注重安全性，但并不是Sendmail不好用，如果真的是这样，Sendmail在Linux发行光盘中早就看不见了。两者各有优点和缺点，管理人员可在两者之间自行取舍。

Sendmail和Postfix切换方式有两种，第一种是System-switch-mail（图形界面），第二种是alternatives --config mta（文字界面）。

### System-switch-mail（图形界面）

Red Hat Linux 7.3 使用 redhat-switchmail软件，Red Hat Linux 9.0 和 Enterprise Linux 3使用redhat-switch-mail软件，Fedora Core 2和Red Hat Enterprise Linux 4使用 system-switch-mail软件。

首先检查是否安装Sendmail和Postfix服务，这样才可以使用切换工具测试。

检查是否安装Sendmail，确定已正确安装并配置Sendmail。

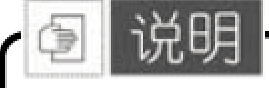
```
[root@localhost ~]# rpm -qa | grep sendmail
sendmail-cf-8.14.4-8.el6.noarch
sendmail-8.14.4-8.el6.x86_64
```

检查是否安装Postfix，确定已正确安装并配置Postfix。

```
[root@localhost ~]# rpm -qa | grep postfix
postfix-2.6.6-2.1.el6_0.x86_64
```

检查是否安装system-switch-mail软件，确定已正确安装system-switch-mail软件。

```
[root@localhost ~]# rpm -qa | grep system-switch-mail system-switch-mail-0.5.25-12.noarch
```




CentOS 5.x默认已安装system-switch-mail软件。

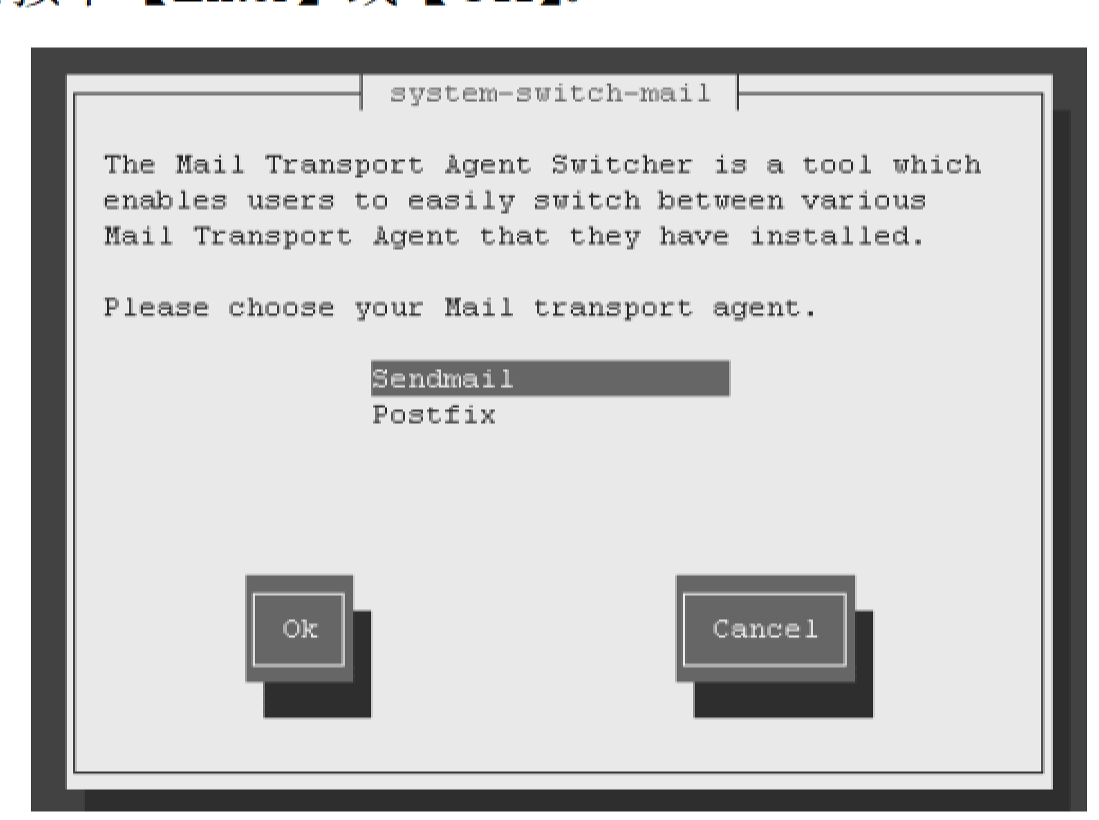
System-switch-mail已经很久没有更新了，不过低版本软件一样可以安装到CentOS 6.x，目前测试可以正常使用。

```
[root@localhost ~]# wget ftp://ftp.nluug.nl/pub/os/Linux/distr/startcom/AS-5.0.0/
os/i386/StartCom/RPMS/system-switch-mail-0.5.25-12.noarch.rpm
…中间省略…
[root@localhost ~]# rpm -ivh system-switch-mail-0.5.25-12.noarch.rpm
warning: system-switch-mail-0.5.25-12.noarch.rpm: Header V3 DSA/SHA1
 Signature, key ID 652e84dc: NOKEY
Preparing...          ########################################### [100%]
   1:system-switch-mail     ######################################### [100%]
```

说明

档案来源：http://rpm.pbone.net/index.php3/stat/4/idpl/8191785/dir/startcom_5/com/system-switch-mail-0.5.25-12.noarch.rpm.html

使用system-switch-mail切换Mail transport agent，界面中会显示Sendmail和Postfix两种MTA，如果只有一种，则代表其中一种MTA未正确安装，请重新安装，输入【system-switch-mail】命令开启工具，打开界面后红色光标指向哪一种MTA，即代表目前以此种MTA运行，选择其中一种切换MTA，然后按下【Enter】或【OK】。




这里Sendmail目前正在启动，Postfix停用，检查目前状态和默认启用状态。检查后Sendmail目前是启动状态，默认也为启用。

```
[root@localhost ~]# service sendmail status//查询 Sendmail 运行状态
sendmail (pid  2045) is running...
sm-client (pid  2053) is running...
[root@localhost ~]# chkconfig --list sendmail  //查询 Sendmail 默认启动状态
sendmail        0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

Postfix目前停用，默认也未启用。

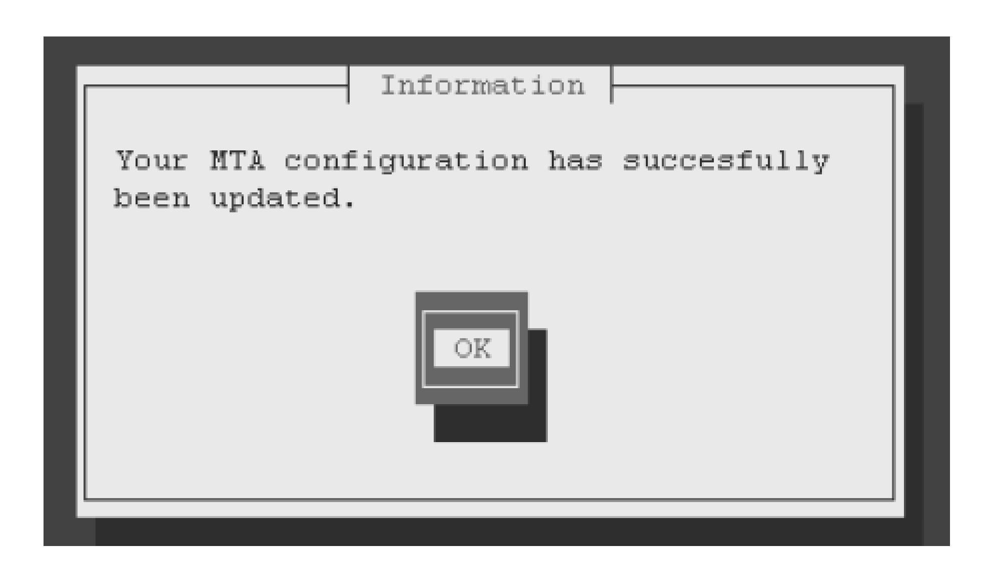
```
[root@localhost ~]# service postfix status    //查询 Postfix 运行状态
master is stopped
[root@localhost ~]# chkconfig --list postfix  //查询 Postfix 默认启动状态
```

```
service postfix supports chkconfig, but is not referenced in any runlevel (run 'chkconfig
--add postfix')
```

若要从Sendmail切换至Postfix，输入【system-switch-mail】，打开system-switch-mail工具，红色光标目前在Sendmail上，将光标移至Postfix，然后按【OK】切换。




下图显示MTA已正确切换，按【OK】，系统会自动启动所切换的MTA服务，另一个服务则会停用。




切换后检查目前服务启动状态，目前Sendmail被停用并且默认启动状态也停用。

```
[root@localhost ~]# service sendmail status         //查询 Sendmail 运行状态
sendmail is stopped
sm-client is stopped
[root@localhost ~]# chkconfig --list sendmail    //查询 Sendmail 默认启动状态
service sendmail supports chkconfig, but is not referenced in any runlevel (run 'chkconfig
--add sendmail')
```

Postfix目前运行状态为启动并且已配置默认启动状态。

```
[root@localhost ~]# service postfix status           //查询 Postfix 运行状态
master (pid  2239) is running...
[root@localhost ~]# chkconfig --list postfix     //查询 Postfix 默认启动状态
postfix          0:off    1:off    2:on    3:on    4:on    5:on    6:off
```

实际操作过后，system-switch-mail工具会自动启动停用服务，并将启动的服务配置为默认启动，停用的服务停用所有默认启动。

## alternatives－config mta（文字界面）

使用文字界面切换也很方便，无需安装，MTA切换只能切换MTA的默认启动，MTA服务状态必须自行启动停用，所以建议尽量使用System-switch-mail。

```
[root@localhost ~]# alternatives --config mta
There are 2 programs which provide 'mta'.
  Selection    Command
-----------------------------------------------
   1           /usr/sbin/sendmail.postfix
*+ 2           /usr/sbin/sendmail.sendmail
Enter to keep the current selection[+], or type selection number:
                                                      //输入 Selection 数字
```

不管用任何方式切换，在切换完毕后，请将不需要的MTA服务停用，以免两种MTA发生冲突。

# 第20章

# OpenWebMail——电子邮箱

OpenWebMail官方网站：http://openwebmail.acatysmoof.com/。

OpenWebMail 试用网站：http://openwebmail.amcpl.net/cgi-bin/openwebmail/openwebmail.pl。

使用默认的Demo用户进入OpenWebMail功能界面。

## OpenWebMail的特点

### 系统部分

- 友好的用户界面。
- 多国语言。
- 多图显示，多种模板，自定义背景。
- 世界时区切换，支持夏令时。
- 多种认证模块（unix，pop3，mysql，postgres，ldap）同时支持PAM认证。
- 用户配额管理模块（quota_unixfs，quota_du），可强制清除超过配额者过旧的邮件或文档。
- 支持虚拟主机/用户别名。
- 支持虚拟用户（能使用pop3/webmail功能，但无须创建unix用户）。
- 支持多个网段，各网段可做不同的配置。
- 支持配置用户权限功能。
- 支持网页压缩传送，提高传输效率。
- 在线更改密码。
- 用户历史记录。
- 配合SpeedyCGI，高效内存利用技术。

### 邮件列表

- 快速切换不同信箱。

- 快速换页功能。
- 可按照邮件状态、邮件日期、发件人、邮件标题、邮件大小排序。
- 可以配置过滤条件，只列出合乎条件的邮件。
- 新邮件语音通知。
- 邮箱变更通知，显示最近各信箱中的邮件。
- 变更邮件读取状态。

**邮件读取**

- 与Outlook接近的多媒体邮件显示功能。
- 多种字符集自动转换（如简繁转换、日文Shif-JIS/ISO-2022-JP/EUC-JP、各种字集/UTF-8）。
- 可收取外部POP3邮件。
- 可关闭邮件中的CGI链接，避免email地址泄漏。
- 可关闭邮件中的Javascript，避免恶意的script程序。
- 可将HTML邮件转换成文字格式显示，完全避免HTML病毒。
- 支持已读回执。
- 支持自动回复。
- 支持邮件重组功能。
- 邮件中的附件可被下载或储存到网络硬盘中。

**邮件撰写**

- 提供HTML邮件编写功能，可内嵌图片、声音、表格，同时支持Windows IE与所有平台上的Mozilla。
- 支持通信组邮件地址。
- 支持写信底稿。
- 支持暂时保存草稿。
- 支持个人通信与公用通信簿。
- 拼写检查。
- 可动态切换邮件内容字符集。
- 可选择发送邮件字符集。
- 可通过本机或外部主机发送邮件。
- 电子邮件中的附件可由网络硬盘添加或由用户上传。

**邮件过滤**

- 可定义个人邮件规则与公用邮件规则。
- 可利用外部程序进行病毒扫描。
- 可利用外部程序进行垃圾邮件分类。
- 支持过滤重复出现过多次的邮件。

- 支持过滤发件人地址格式不正确的邮件。
- 支持过滤伪造来源IP地址邮件。
- 支持过滤伪造发信人的邮件。
- 支持过滤伪造EXE程序的附件。

### 邮件搜索

- 可针对发信人、收信人、邮件主题、邮件标题、邮件内容、附件名称进行全文检索。
- 同时搜索多个邮箱
- 支持正则表达式（Regular Expression）。
- 搜索时可根据需要，自动进行内码转换后再进行对比（eg: 以简体字搜寻繁体邮件）。

### 邮件管理

- 邮箱的创建/重命名/删除/下载。
- 邮件的复制/移动/删除/下载。
- 重建/修复邮箱索引。
- 自动清除垃圾桶内N天以上的邮件。

### 计划任务

- 年/月/周/日计划任务列表。
- 全年计划任务列表。
- 支持个人计划任务与公用计划任务。
- 可配置周期性计划任务。
- 计划任务可标明色彩。
- 计划任务相关Link可以是外部URL或是OpenWebMail中出现的任何Link，如邮箱中的某封邮件或网络硬盘上的某个文件。
- 与电子邮件列表主画面结合，提供计划任务提醒功能。
- 计划任务提醒也可以发送给外部邮件地址，转移到其他装置上。

### 网络硬盘

- 以用户home目录作为网络硬盘目录。
- 目录与文件的基本操作有新增/复制/移动/删除（包含子目录）。
- 文件的上传与下载。
- 多文件或目录下载（实时压缩文件传输）。
- 文本文件在线编辑。
- HTML文件实时预览（文件不一定在public_htm下）。
- 创建压缩文件/解压缩/内容列表。
- 图片位图功能。
- 文件搜索，可搜索文件名或文字内容。
- 电子邮件中的附件可由网络硬盘添加，也可储存到网络硬盘中。

# 20.1 安装OpenWebMail 3.0

OpenWebMail的安装方式有别于以往，OpenWebMail 2.53版可以使用yum在线更新的方式安装，不过3.0后又回到最一开始的源码编译安装方式，步骤也变得比较繁琐，所以务必都不要略过不要略过每一个操作，以免安装失败。

安装OpenWebMail前必须要先确认已安装Dovecot收信软件POP3或SMTP和发信软件Sendmail或Postfix、Web网站软件Apache等服务，把它们设置为默认开机启动，并在防火墙配置中开启相对应的端口（25、80、110），所有都确认完成后，就可以开始安装OpenWebMail必备软件了。

## 安装必备软件

OpenWebMail以前只要安装Perl-Text-Iconv即可，不过OpenWebMail 3.0版本之后，必须要安装更多的软件，因为OpenWebMail是由perl语法写成的，所以除了GCC外，大部分的软件都与perl有关，perl的软件有很多，基本上我们只要安装perl-CGI、perl-YAML、perl-CPAN、perl-suidper l即可，建议使用yum在线更新方式安装，如果不想输入太多命令，可以直接输入perl*，其实很多初学者都会这样安装，不过不建议这样做。

```
[root@localhost ~]# yum install -y gcc perl-Text-Iconv perl-CGI perl-YAML perl-CPAN
perl-suidperl httpd
Dependencies Resolved
=========================================================================
 Package   Arch     Version        Repository     Size
=========================================================================
Installing:
 Gcc                 x86_64      4.4.4-13.el6          base   10 M
 Httpd               x86_64   2.2.15-5.el6.centos   base      811 k
 perl-CGI            x86_64   3.49-115.el6          base      191 k
 perl-Text-Iconv     x86_64   1.7-6.el6             base      22 k
 perl-YAML           noarch   0.70-4.el6            base      81 k
 perl-suidperl       x86_64   4:5.10.1-115.el6      base      46 k
Installing for dependencies:
 Apr                 x86_64   1.3.9-3.el6_0.1       updates   124 k
 apr-util            x86_64   1.3.9-3.el6_0.1       updates   87 k
 apr-util-ldap       x86_64   1.3.9-3.el6_0.1       updates   15 k
 cloog-ppl           x86_64    0.15.7-1.2.el6       base      93 k
 cpp                 x86_64    4.4.4-13.el6         base      3.7 M
 glibc-devel         x86_64    2.12-1.7.el6_0.5     updates   961 k
 glibc-headers       x86_64    2.12-1.7.el6_0.5     updates   592 k
 httpd-tools         x86_64    2.2.15-5.el6.centos  base      68 k
 kernel-headers      x86_64    2.6.32-71.29.1.el6   updates   991 k
 mpfr                x86_64    2.4.1-6.el6          base      157 k
 ppl                 x86_64    0.10.2-11.el6        base      1.3 M
Updating for dependencies:
 glibc               x86_64    2.12-1.7.el6_0.5     updates   3.7 M
```

```
 glibc-common      x86_64    2.12-1.7.el6_0.5       updates   14 M
Transaction Summary
======================================================================
Install      17 Package(s)
Upgrade       2 Package(s)
Total download size: 37 M
```

## 安装OpenWebMail 3.0

安装完OpenWebMail必备软件后，就可以开始安装OpenWebMail 3.0版本了，其安装步骤和以前的版本不太一样，需要编辑源代码文件进行安装，所以千万不要遗漏某个步骤，尤其是权限的设置，这影响到是否可以安装成功。

此安装方式参考了官方的Fedora 14的安装方式，有些步骤不一样，其他配置基本相同。

首先创建要存放OpenWebMail压缩文件的目录，解压缩后会将相应的目录拷贝至指定目录，所以建议创建一个目录解压缩后再拷贝，以免出错。

```
[root@localhost ~]# mkdir /tmp/openwebmail  //创建 openwebmail 压缩文件目录
[root@localhost ~]# cd /tmp/openwebmail     //切换到 openwebmail 压缩文件目录
[root@localhost openwebmail]#               //正确切换到 openwebmail 压缩文件目录
```

使用wget命令下载OpenWebMail压缩文件，目前官方网站有有两个压缩文件，一个是beta版本，一个是预发行版本，不过建议下载openwebmail-current.tar.gz版本，此文件是准备发行的版本。

```
[root@localhost openwebmail]# wget
http://openwebmail.acatysmoof.com/download/current/openwebmail-current.tar.gz
```

> 说明
>
> openwebmail-current.tar.gz最新发行版的文件来源为http://openwebmail.acatysmoof.com/download/current/。

下载完成后，在OpenWebMail解压缩目录中解压下载好的OpenWebMail预发行版本的压缩文件。

```
[root@localhost openwebmail]# tar -xvzBpf openwebmail-current.tar.gz
```

解压OpenWebMail压缩文件后有两个目录，分别是cgi-bin及data目录，这两个目录内都会有一个OpenWebMail目录，不过这两个目录的内容不一样，cgi-bin是OpenWebMail主程序，data是OpenWebMail所要使用的相关图片或软件，先将cgi-bin目录移动到网页cgi默认目录，接下来把data目录移动到两个目录中，不过解压缩后只有一个data目录，所以先复制再移动，先将data内的OpenWebMail复制到网页默认路径，如果只做此操作，在浏览器打开OpenWebMail后，所有图片都不会显示，最后再将data目录移动到/var/www目录下。

```
[root@localhost openwebmail]# mv cgi-bin/openwebmail /var/www/cgi-bin/
[root@localhost openwebmail]# cp -r data/openwebmail /var/www/html
[root@localhost html]# mv data /var/www
```

说明

登录时若出现Software error错误信息，代表/var/www下没有data目录，未将压缩文件内的data目录移动至/var/www目录，所以以上每一个步骤都不能缺少。

```
Software error:
/var/www/data/openwebmail/layouts/classic/templates/shared_error.tmpl does
not exist. No error messages can be displayed. at
/var/www/cgi-bin/openwebmail/shares/ow-shared.pl line 1158.
For help, please send mail to the webmaster (root@localhost), giving this error
message and the time and date of the error.
```

确定复制完成后，先进入OpenWebMail主程序网页目录，然后将OpenWebMail解压缩目录删除，也可以在完成安装后再删除，以免有遗漏的文件。

```
[root@localhost openwebmail]# cd /var/www/cgi-bin/openwebmail
[root@localhost openwebmail]# rm -rf /tmp/openwebmail
                                              //删除 OpenWebMail 压缩文件
```

将OpenWebMail几个目录内的pl文件权限配置为777，再将wrapsuid.pl设为660，一定要配置此权限，否则会无法打开OpenWebMail登录界面。

```
[root@localhost openwebmail]# chmod
777 ./misc/tools/wrapsuid/wrapsuid.pl ./misc/tools/wrapsuid/wrapsuid.pl
/var/www/cgi-bin/openwebmail/openwebmail*.pl
[root@localhost openwebmail]# chmod 660 ./misc/tools/wrapsuid/wrapsuid.pl
```

将OpenWebMail主程序目录下的pl文件权限都配置为4755，不要怀疑就是4755！

```
[root@localhost openwebmail]# chmod 4755 openwebmail*.pl
```

再将suidperl权限配置为4555，这也不要怀疑就是4555！若没有文件可以配置表示没有安装perl-suidperl，可以使用YUM在线更新安装方式安装，安装完成后，再来配置权限。

```
[root@localhost openwebmail]# chmod 4555 /usr/bin/suidperl
```

说明

如果没有配置以上文件权限，可能会出现Internal Server Error错误信息

**Internal Server Error**

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, root@localhost and inform them of the time the error occurred, and anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

---

*Apache/2.2.15 (CentOS) Server at 192.168.233.235 Port 80*

说明

若出现【以下脚本必须设置为root权限才能读取系统文件夹：/var/www/cgi-bin/openwebmail/openwebmail.pl】，表示没有对/usr/bin/suidperl设置权限。

创建OpenWebMail的日志文件，并设置日志文件权限。

```
[root@localhost openwebmail]# touch /var/log/openwebmail.log
[root@localhost openwebmail]# chown root:mail /var/log/openwebmail.log
```

复制网页默认目录下OpenWebMail目录内的redirect.html至网页索引目录，并将文件名修改成index.html，此文件内创建了快捷访问连接，以免使用者还要输入太长的网址。

```
[root@localhost openwebmail]# cp -p /var/www/html/openwebmail/redirect.html
/var/www/html/index.html
```

接下来编辑OpenWebMail配置文件，要设置相关目录的路径，一般要修改两个路径，分别是ow_cgidir和ow_htmldir，ow_cgidir是cgi网页默认目录，ow_htmldir是网页数据目录，目前两个目录都在/var/www下，所以可进行修改。

```
[root@localhost openwebmail]# vi etc/openwebmail.conf
# This file sets options for all domains and all users.
# To set options on per domain basis, please put them in sites.conf/domainname
# To set options on per user basis, please put them in users.conf/username
#
# Please refer to openwebmail.conf.help for the description of each option
#
domainnames             auto
auth_module             auth_unix.pl
mailspooldir            /var/mail
ow_cgidir               /var/www/cgi-bin/openwebmail
                                                        //OpenWebMail 主程序路径
ow_cgiurl               /cgi-bin/openwebmail
ow_htmldir              /var/www/data/openwebmail    //OpenWebMail 数据路径
ow_htmlurl              /openwebmail
logfile                 /var/log/openwebmail.log
```

将身份认证配置文件复制到OpenWebMail主程序目录内的etc目录下。

```
[root@localhost openwebmail]# cp etc/defaults/auth_unix.conf etc/
```

修改身份认证配置文件，只修改passwdfile_encrypted及passwdmkdb参数，其他不用修改。

```
[root@localhost openwebmail]# vi etc/auth_unix.conf
# change_smbpasswd
# ---------------------------------------------------------------------
# if this option is set to yes, openwebmail will also change the
# smbpasswd after changing the unix password successfully
passwdfile_plaintext    /etc/passwd
passwdfile_encrypted    /etc/shadow
passwdmkdb              none
```

将dbm文件复制至OpenWebMail主程序目录内的etc目录下。

```
[root@localhost openwebmail]# cp etc/defaults/dbm.conf etc/
```

更新dbm配置文件，修改dbmopen_ext及dbmopen_haslock参数，其他不修改。

```
[root@localhost openwebmail]# vi etc/dbm.conf
# dbmopen_haslock
# ------------------------------------------------------------------
# If your perl dbm system will do filelock in dbmopen () by itself,
# set this option to 'yes' so openwebmail won't do unnecessary filelock
# before dbmopen. On most systems, this option should be set to 'no'.
#
# ps: If your openwebmail hangs after login or saving preference,
#     you probably need to set this option to 'yes'
dbm_ext                  .db
dbmopen_ext              .db
dbmopen_haslock           no
```

说明

若CentOS操作系统按照官方步骤安装，就会发生错误，无法初始化。

```
[root@localhost openwebmail]# ./openwebmail-tool.pl --init
Please change './etc/dbm.conf' from
dbm_ext                  .pag     //此三行为官方配置 Fedora 方式，会发生错误
dbmopen_ext              none
dbmopen_haslock          no
to
dbm_ext                  .db     //必须修改成此三行，初始化才能成功
dbmopen_ext              .db
dbmopen_haslock          no
And execute './openwebmail-tool.pl --init' again!
ps: If you are running openwebmail in persistent mode,
    don't forget to 'touch openwebmail*.pl', so speedycgi
    will reload all scripts, modules and conf files in --init.
```

## 初始化OpenWebMail 服务

一切配置完成后，就可以初始化OpenWebMail服务了，和以前版本的初始化方法不一样，执行命令很快就会结束，随后询问是否显示成功安装信息，可根据需求配置。

```
[root@localhost openwebmail]# ./openwebmail-tool.pl --init
creating db /var/www/cgi-bin/openwebmail/etc/maps/b2g ...done.
creating db /var/www/cgi-bin/openwebmail/etc/maps/g2b ...done.
creating db /var/www/cgi-bin/openwebmail/etc/maps/lunar ...done.
Welcome to OpenWebMail!
This program is going to send a short message back to the developers
to give us statistics for future development. The content to be sent is:
OS: Linux 2.6.32-71.el6.x86_64 x86_64
Perl: 5.010001
WebMail: OpenWebMail 3.00_beta4 20110808 revision 603
Send the site report? (Y/n) y                          //是否显示成功安装信息
sending report...
report sent successfully.
```

```
Show your support for OpenWebMail on Ohloh:
http://www.ohloh.net/p/openwebmail
```

初始化完成后，打开OpenWebMail登录界面前先执行以下命令，否则无法登录，注意命令执行后，会要求输入【yes】，按取消的话，再次执行时，就要一行一行回答，大约需要几分钟才能完成，完成后重新刷新网页即可以正常使用。

```
[root@localhost openwebmail]# perl -MCPAN -e 'install HTML::Template'
```

说明

以下错误信息需要执行【perl -MCPAN -e 'install HTML::Template'】命令

```
Software error:
Can't locate HTML/Template.pm in @INC (@INC contains:
/usr/local/lib64/perl5 /usr/local/share/perl5
/usr/lib64/perl5/vendor_perl /usr/share/perl5/vendor_perl
/usr/lib64/perl5 /usr/share/perl5) at
/var/www/cgi-bin/openwebmail/openwebmail-main.pl line 60.
BEGIN failed--compilation aborted at
/var/www/cgi-bin/openwebmail/openwebmail-main.pl line 60.
For help, please send mail to the webmaster (root@localhost), giving this
error message and the time and date of the error.
```

## 创建邮箱用户

登录OpenWebMail前，由于新创建的邮件服务器没有任何的用户可以登录，所以必须创建至少一个用户，才可以测试是否可以正常登录，这里创建一个用户jerry，并配置密码。

```
[root@localhost openwebmail]# adduser jerry   //新增用户 jerry
[root@localhost openwebmail]# passwd jerry    //配置新用户密码
Changing password for user jerry.
New password:                                 //第一次输入密码
BAD PASSWORD: it is too simplistic/systematic
Retype new password:                          //再次输入密码
passwd: all authentication tokens updated successfully.
```

## 重新启动Apache服务

OpenWebMail安装完成后，由于一部分设置与Apache服务有关，建议重新启动Apache服务，OpenWebMail服务才能正常使用。

```
[root@localhost openwebmail]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

## 使用OpenWebMail登录

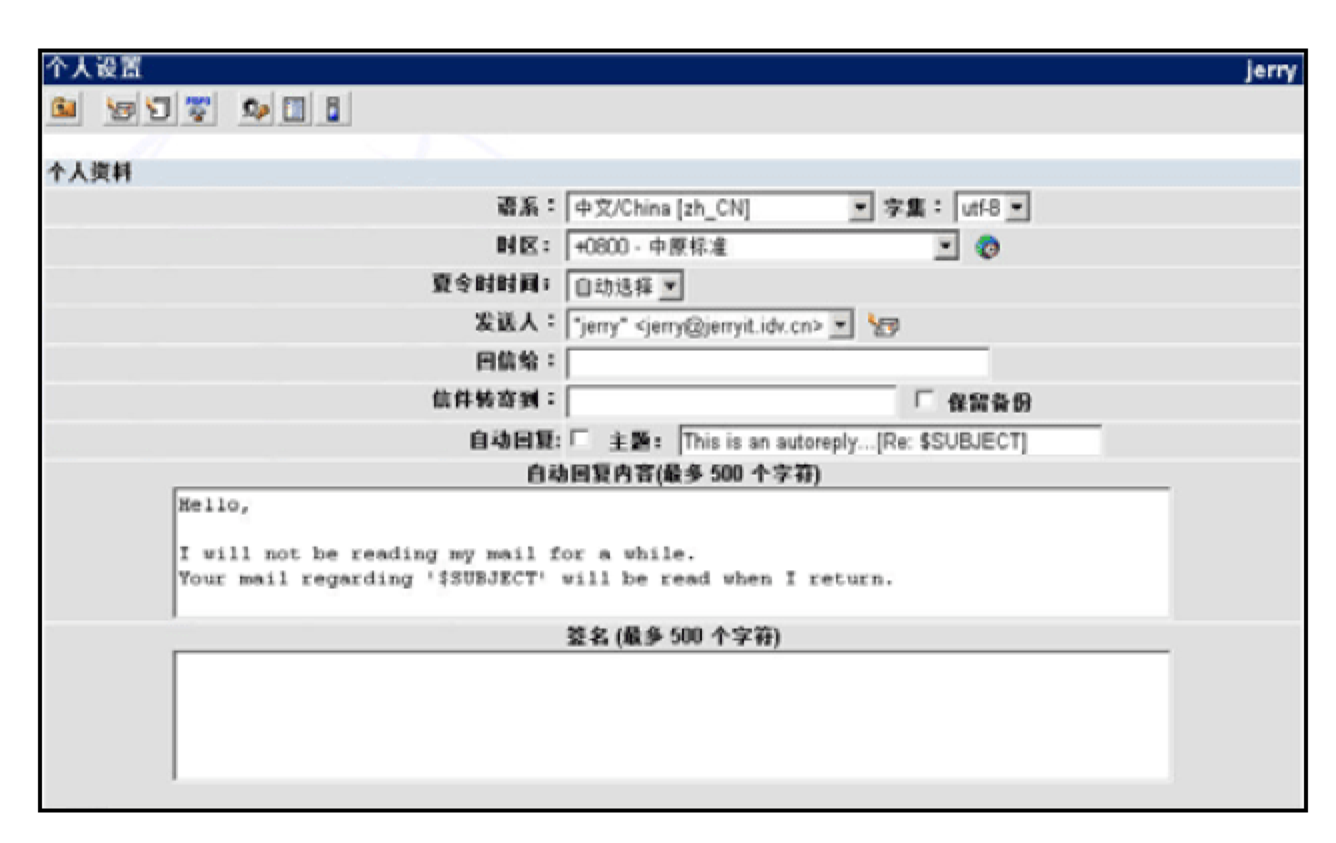
所有设置就绪后，就可以使用OpenWebMail登录了，由于创建了转址网页，只需输入【http://网址或IP地址】，就会帮你转至OpenWebMail登录画面，不用输入【http://网址或IP地址/cgi-bin/openwebmail/openwebmail.pl】这么长的网址。输入刚创建的邮箱用户jerry，输入用户密码后，按【登录】。




第一次登录OpenWebMail后会显示欢迎使用画面，并要求做一些基本的配置，按【继续】。




在【个人设置】中设置好【夏令时时间】和【语系】就可以先进入OpenWebMail，其他配置可以以后设置。




保存OpenWebMail个人设置，按【继续】。



进入OpenWebMail邮件信箱主画面，可以开始使用信箱了！



## 20.2 安装OpenWebMail 2.53版本

安装OpenWebMail 2.53版本前必须要先确认已安装Dovecot收信软件POP3或SMTP和发信软件Sendmail或Postfix、Web网站软件Apache等服务，把这几个服务设置为默认开机启动，并在防火墙配置中开启相对应的端口（25、80、110），所有都确认完成后，就可以开始安装OpenWebMail必备软件了。

### 安装perl-Text-Iconv

在安装OpenWebMail软件前，还有一个软件要安装，那就是perl-Text-Iconv，此软件无法使用YUM在线更新方式安装，必须自行下载rpm进行安装，下载完毕后，可立即安装perl-Text-Iconv。

```
[root@localhost ~]# wget http://openwebmail.org/openwebmail/download/
redhat/rpm/packages/centos5/perl-Text-Iconv/i386/
perl-Text-Iconv-1.7-2.el5.i386.rpm
…中间省略…
[root@localhost ~]# rpm -ivh perl-Text-Iconv-1.7-2.el5.i386.rpm
Preparing...                ########################################### [100%]
   1:perl-Text-Iconv        ########################################### [100%]
```

> **说明**
>
> perl-Text-Iconv 文件来源为 http://openwebmail.org/openwebmail/download/redhat/rpm/packages/centos5/perl-Text-Iconv/。

### 创建openwebmail使用yum的repo

先将目录切换到yum.repos.d下，利用lftpget命令下载openwebmail.repo文件，检查有没有正常下载openwebmail.repo到目录内。

```
[root@localhost ~]# cd /etc/yum.repos.d
[root@localhost yum.repos.d]# lftpget
http://openwebmail.org/openwebmail/download/redhat/rpm/release/openwebmail.repo
```

```
[root@localhost yum.repos.d]# ll
total 44
-rw-r--r-- 1 root root 1926 Feb  8  2011 CentOS-Base.repo
-rw-r--r-- 1 root root  631 Feb  8  2011 CentOS-Debuginfo.repo
-rw-r--r-- 1 root root  626 Feb  8  2011 CentOS-Media.repo
-rw-r--r-- 1 root root 4663 Feb  8  2011 CentOS-Vault.repo
-rw-r--r-- 1 root root  323 May 29  2008 openwebmail.repo
```

## 使用YUM安装OpenWebMail

一切必备软件安装完成后，就可以安装OpenWebMail软件了，使用YUM在线更新方式进行安装，系统会自动安装OpenWebMail软件及相关软件，如openwebmail-data、perl软件的perl-Compress-Zlib及perl-suidperl。

```
[root@localhost ~]# yum install -y openwebmail    //安装 OpenWebMail
Dependencies Resolved
========================================================================
 Package               Arch       Version            Repository          Size
========================================================================
Installing:
 openwebmail           i386       2.53-3              openwebmail       2.4 M
Installing for dependencies:
 openwebmail-data      i386       2.53-3              openwebmail       7.3 M
 perl-Compress-Zlib    i386       1.42-1.fc6          base               52 k
 perl-suidperl         i386       4:5.8.8-32.el5_6.3 updates             62 k
Updating for dependencies:
 perl                  i386       4:5.8.8-32.el5_6.3 updates             12 M
Transaction Summary
========================================================================
Install       4 Package(s)
Upgrade       1 Package(s)
Total download size: 21 M
```

说明

如果无法输入【yum install openwebmail】安装的话，则代表/etc/yum.repos.d中没有openwebmail.repo文件。

## 初始化OpenWebMail

安装完OpenWebMail软件后，OpenWebMail需要初始化才可以使用，执行一下命令系统就会开始初始化，初始化完成前会询问是否要将信息上传，基本上都是按y同意。

```
[root@localhost ~]# /var/www/cgi-bin/openwebmail/openwebmail-tool.pl --init
creating db /var/www/cgi-bin/openwebmail/etc/maps/b2g ...done.
creating db /var/www/cgi-bin/openwebmail/etc/maps/g2b ...done.
```

```
creating db /var/www/cgi-bin/openwebmail/etc/maps/lunar ...done.
Creating UTF-8 locales...
langconv ar_AE.CP1256 -> ar_AE.UTF-8
langconv ar_AE.ISO8859-6 -> ar_AE.UTF-8
langconv bg_BG.CP1251 -> bg_BG.UTF-8
langconv ca_ES.ISO8859-1 -> ca_ES.UTF-8
langconv cs_CZ.ISO8859-2 -> cs_CZ.UTF-8
langconv da_DK.ISO8859-1 -> da_DK.UTF-8
langconv de_DE.ISO8859-1 -> de_DE.UTF-8
langconv el_GR.ISO8859-7 -> el_GR.UTF-8
langconv en_US.ISO8859-1 -> en_US.UTF-8
langconv es_AR.ISO8859-1 -> es_AR.UTF-8
langconv fi_FI.ISO8859-1 -> fi_FI.UTF-8
langconv fr_FR.ISO8859-1 -> fr_FR.UTF-8
langconv he_IL.CP1255 -> he_IL.UTF-8
langconv hr_HR.ISO8859-2 -> hr_HR.UTF-8
langconv hu_HU.ISO8859-2 -> hu_HU.UTF-8
langconv id_ID.ISO8859-1 -> id_ID.UTF-8
langconv it_IT.ISO8859-1 -> it_IT.UTF-8
langconv ko_KR.eucKR -> ko_KR.UTF-8
langconv lt_LT.CP1257 -> lt_LT.UTF-8
langconv nl_NL.ISO8859-1 -> nl_NL.UTF-8
langconv no_NO.ISO8859-1 -> no_NO.UTF-8
langconv pl_PL.ISO8859-2 -> pl_PL.UTF-8
langconv pt_BR.ISO8859-1 -> pt_BR.UTF-8
langconv pt_PT.ISO8859-1 -> pt_PT.UTF-8
langconv ro_RO.ISO8859-2 -> ro_RO.UTF-8
langconv ru_RU.KOI8-R -> ru_RU.UTF-8
langconv sk_SK.ISO8859-2 -> sk_SK.UTF-8
langconv sl_SI.CP1250 -> sl_SI.UTF-8
langconv sr_CS.ISO8859-2 -> sr_CS.UTF-8
langconv sv_SE.ISO8859-1 -> sv_SE.UTF-8
langconv th_TH.TIS-620 -> th_TH.UTF-8
langconv tr_TR.ISO8859-9 -> tr_TR.UTF-8
langconv uk_UA.KOI8-U -> uk_UA.UTF-8
...done.
Welcome to the OpenWebMail!
This program is going to send a short message back to the developer,
so we could have the idea that who is installing and how many sites are
using this software, the content to be sent is:
OS: Linux 2.6.18-238.el5 i686
Perl: 5.008008
WebMail: OpenWebMail 2.53 20080123
Send the site report? (Y/n) y            //是否上传信息
sending report...
Thank you.
[root@localhost ~]#
```

## 创建邮件用户

登录OpenWebMail前，由于新创建的邮件服务器没有任何的用户可以登录，所以必须创建至少一个用户，测试是否可以正常登录，这里创建一个用户jerry，并配置密码。

```
[root@localhost ~l]# adduser jerry          //新增用户 jerry
[root@localhost ~l]# passwd jerry           //配置新用户密码
Changing password for user jerry.
New password:                               //第一次输入密码
BAD PASSWORD: it is too simplistic/systematic
Retype new password:                        //再次输入密码
passwd: all authentication tokens updated successfully.
```

## 重新启动Apache服务

OpenWebMail安装完成后，由于一部分设置与Apache服务有关，建议重新启动Apache服务，OpenWebMail服务才能正常使用。

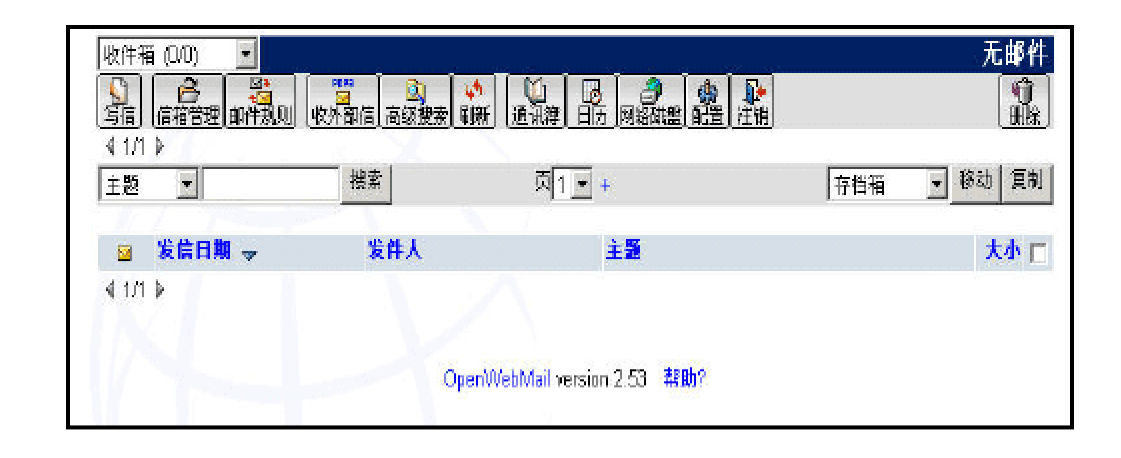
```
 [root@localhost ~]# service httpd restart
Stopping httpd:                                           [  OK  ]
Starting httpd:                                           [  OK  ]
```

## 开始使用OpenWebMail 2.53

打开浏览器，输入【http://IP或网址/cgi-bin/openwebmail/openwebmail.pl】，下图为OpenWebMail登录画面，输入新创建的用户和用户密码登录。




登录后的界面如下，与一般web mail功能相似。



## 20.3 配置域名

OpenWebMail默认设置发件人的域名，若没有配置，默认取本机名称localhost.localdomain，这样发送过去对方也看不出来，还会被当为垃圾邮件。




所以必须配置真正的域名，默认为auto，将域名auto修改成jerryit.idv.cn。

```
[root@localhost ~]# vi /var/www/cgi-bin/openwebmail/etc/openwebmail.conf
#
# Open WebMail configuration file
#
# This file contains just the overrides from defaults/openwebmail.conf,
# please make all changes to this file.
#
# This file sets options for all domains and all users.
# To set options on per domain basis, please put them in sites.conf/domainname
# To set options on per user basis, please put them in users.conf/username
#
# Please refer to openwebmail.conf.help for the description of each option
#
domainnames              jerryit.idv.cn        //默认为 auto，配置所需域名
auth_module              auth_unix.pl
```

配置好域名后，必须要重新启动Apach服务才可以生效。

```
[root@localhost ~]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

重新进入OpenWebMail，就会挂上jerryit.idv.cn的域名。




## 20.4 更换邮箱Logo

OpenWebMail默认首页图片Logo如下图所示，通常创建好后，公司一般会更换为自己的Logo，以显示出公司的特有文化。




## 上传要更换的Logo图片

使用WinSCP工具将更换的Logo上传到OpenWebMail程序的images目录下，示例中Logo文件名为jerry_it.gif。

2.53以前版本images路径：/var/www/data/openwebmail/images/openwebmail.gif。

3.0版本images路径：/var/www/html/openwebmail/images/system/openwebmail.png。

OpenWebMail 2.53版本需要编辑OpenWebMail配置文件，在logo_url参数中，%ow_htmlurl%路径是指/var/www/data/openwebmail，logo图片存放路径是images目录里，默认Logo文件名为openwebmail.gif。这里Logo文件名为jerry_it.gif，在openwebmail.conf配置文件中修改为jerry_it.gif，然后保存退出。

```
[root@localhost ~]# vi /var/www/cgi-bin/openwebmail/etc/openwebmail.conf
logo_url                        %ow_htmlurl%/images/jerry_it.gif
logo_link                       http://openwebmail.org
```

**说明**

%ow_htmlurl%路径为/var/www/data。

3.0版本不需要添加logo_url参数，只要将图片上传到images目录，并将文件名修改成openwebmail.png，重新刷新页面即会加载图片，记得只支持png图片格式，其他不支持。

重新刷新页面后，首页Logo图标就会出现示例Logo的图片，如下图所示。



## 修改Logo的超链接

首页Logo图示有一个超链接，默认为OpenWebMail官网（http://openwebmail.org），可在OpenWebMail配置文件中自行修改链接。

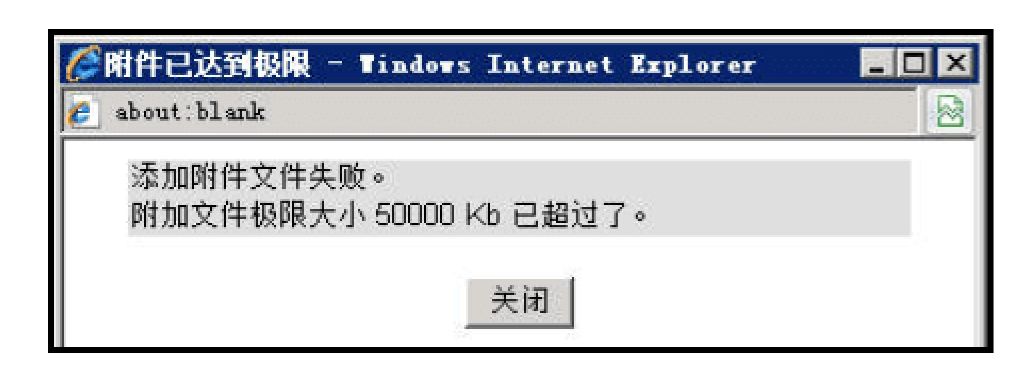
```
[root@localhost ~]# vi /var/www/cgi-bin/openwebmail/etc/openwebmail.conf
logo_url                    %ow_htmlurl%/images/openwebmail.gif
logo_link         http://www.jerryit.idv.cn/jerry710822/      //修改连接
```

# 20.5 配置附件文件容量

电子邮件中的附加文件是很重要的一环，不过附加文件太大对邮件主机是一种负荷，通常用户发送邮件时，附加文件不需要很大，所以可将附加文件最大容量配置得小一点，OpenWebMail默认附加文件最大容量为50MB，如右图所示。




附加文件若超过默认的50MB容量，会出现警告信息，如右图所示。




## 配置附加文件容量

编辑OpenWebMail配置文件，修改attlimit参数，配置附加文件最大容量为10MB，建议实际附加文件约3~5MB就好，再大就对邮件服务器功能存影响了。

```
[root@localhost ~]# vi /var/www/cgi-bin/openwebmail/etc/openwebmail.conf
attlimit                 10000
```

重新加入附加文件，显示附加文件的最大容量为10MB。



OpenWebMail配置附加文件容量，其实也跟Sendmail及Postfix服务接收的邮件容量有关，只要收发邮件服务器都将容量配置为2MB，不管附加文件容量配置为10MB还是更大，也是无法发送的，所以配置完成后，记得检查Sendmail的MaxMessageSize参数及Postfix的message_size_limit参数，以免无法发送邮件。

# 20.6 设置个人配置

OpenWebMail的个人配置选项，可以根据个人喜好进行配置，不过有些功能若不让用户使用的话，就必须将其关闭。




编辑OpenWebMail配置文件，默认参数都为yes，若要设为不显示，可将yes改成no，这样就不会出现在个人配置选项中，如以下配置所示，OpenWebMail 3.0配置文件必须自行输入，以下为参考OpenWebMail 2.53配置文件。

```
[root@localhost ~]# vi /var/www/cgi-bin/openwebmail/etc/openwebmail.conf
##############################################
# Buttons :
# EditFroms | EditStationary | POP3Setup | ChangePassword | History | Info
enable_editfrombook                yes
enable_stationery                  yes
enable_pop3                        yes
enable_changepwd                   yes
enable_history                     yes
enable_about                       yes
################################################
```

| 项目 | 说明 |
|---|---|
| enable_editfrombook<br>编辑发信地址簿 | 发信地址簿的功能是可以将其他电子邮件发件人添加到地址簿内，发信时在地址簿内选择其中一个当作发件人，收件者就会以为是其他发件人发送，不过发送的邮件还是通过真正用户发送的，这算是一种伪造方式 |
| enable _stationery<br>编辑信纸 | 需要大量回信，而且回复相同的内容时，可以预先写好要回信的内容模板，在回信时选择回信底稿，这样就可以节省不少回信时间 |
| enable _pop3 设定外部邮件 | 可以支持用户收取其他 POP3 邮件主机的邮件 |
| enable _changepwd 修改密码 | 修改邮件用户密码 |
| enable _history 历史记录 | 记录该邮件用户所有的操作记录 |
| enable _about 关于 | 关于邮件主机的系统信息，笔者建议关闭 |

# 20.7 允许用户root登录

OpenWebMail默认root用户是不可以登录的。其实很多系统都不允许使用root用户操作，原因是root权限太大了，一旦被知道，安全性就会受到很大威胁，不过提出要如何使用root登录，是因为很多系统邮件都是寄给root用户的，以方便用户读取邮件，其实可以手动删除，因此建议尽量不要开启root用户登录。




## 配置允许root用户登录

编辑OpenWebMail配置文件，最后一行添加allowed_rootloginip参数，将其设为all，这样就可以允许任何IP地址使用root用户登录了，建议将all改成允许用root登录IP地址，这样比较安全。

```
[root@localhost ~]# vi /var/www/cgi-bin/openwebmail/etc/openwebmail.conf
enable_viruscheck          no
enable_spamcheck           no
enable_learnspam           no
allowed_rootloginip        all
```

## 测试root用户登录

测试是否已允许root用户登录，正常登录后，在新邮件中就可以看到发件人为root用户。




# 20.8 检查日志文件

管理OpenWebMail服务不外乎就是检查日志文件，OpenWebMail日志文件存放路径为/var/log/openwebmail.log，若要改变日志文件存放路径，可以修改OpenWebMail配置文件，在logfile这一行可以看到日志文件存放路径，可以依需求修改。

```
[root@localhost ~]# vi /var/www/cgi-bin/openwebmail/etc/openwebmail.conf
#
domainnames             auto
auth_module             auth_unix.pl
mailspooldir            /var/mail
ow_cgidir               /var/www/cgi-bin/openwebmail
ow_cgiurl               /cgi-bin/openwebmail
ow_htmldir              /var/www/data/openwebmail
ow_htmlurl              /openwebmail
logfile                 /var/log/openwebmail.log
                                    //OpenWebMail 日志文件存放路径
```

检查OpenWebMail日志文件，输入【cat /var/log/openwebmail.log】查看，这样OpenWebMail可以清楚了解是如何运作的。

```
Fri Sep  7 00:46:51 2012 - [2596] (192.168.233.1) jerry - login - jerry*192.168.233.
235-session-0.53521678720517б - active=0,2,4
Fri Sep  7 00:47:09 2012 - [2598] (192.168.233.1) jerry - move message - move 10 msg
s from INBOX to mail-trash - ids=<20120906164517.M322@jerryit.idv.cn>, <201209061645
09.M26097@jerryit.idv.cn>, <20120906164504.M14521@jerryit.idv.cn>, <20120906164459.M
27429@jerryit.idv.cn>, <20120906164453.M45852@jerryit.idv.cn>, <20120906164448.M8824
7@jerryit.idv.cn>, <20120906164443.M53204@jerryit.idv.cn>, <20120906163805.M11664@ma
il.jerryit.idv.cn>, <20120906163503.M51567@mail.jerryit.idv.cn>, <20120906163458.M93
772@mail.jerryit.idv.cn>
Fri Sep  7 00:47:31 2012 - [2600] (192.168.233.1) jerry - move message - move 1 msgs
 from INBOX to mail-trash - ids=<20120906163451.M78993@mail.jerryit.idv.cn>
Fri Sep  7 00:47:48 2012 - [2603] (192.168.233.1) jerry - emptyfolder - mail-trash
Thu Sep  6 16:48:14 2012 - [2606] (192.168.233.1) jerry - send message - trying to c
onnect to smtp server 0.0.0.0:25
Thu Sep  6 16:48:14 2012 - [2606] (192.168.233.1) jerry - send message - connected t
o smtp server 0.0.0.0:25
Thu Sep  6 16:48:14 2012 - [2606] (192.168.233.1) jerry - send message - subject=tes
t - to=tom@jerryit.idv.cn
Fri Sep  7 00:48:19 2012 - [2612] (192.168.233.1) jerry - logout - jerry*192.168.233
.235-session-0.535216787205176
Fri Sep  7 00:48:26 2012 - [2614] (192.168.233.1) jerry - login error - auth_unix.pl
, ret -4, Password incorrect
```

日志文件中很多参数都有意义，通过下表可以了解OpenWebMail日志文件常用信息。

| OpenWebMail 日志文件说明 | |
|---|---|
| **操作说明** | **操作信息** |
| 日志时间 | Fir Sep 7 00:46:51 2012 |
| 日志编号 | 2596 |
| 用户登录计算机 IP | 192.168.233.1 |
| 用户登录 | login |
| 登录用户 | jerry |
| 删除到垃圾桶 | clean trash |
| 移到邮件 | move message |
| 清理垃圾桶 | emptyfolder |
| 发送邮件 | sendmessage |
| 用户注销 | logout |
| 用户登录失败 | login error |
| 邮件主题 | subject= |
| 收件者 | to= |

# 第21章

# SPAM——垃圾邮件

电子邮件是人人都会用到的工具，每天打开信箱就会有很多信件，不过真正有效的信件只有几封，其余大多都是垃圾邮件，对垃圾邮件（英语为spam）现在还没有一个非常严格的定义，一般来说，凡是未经用户许可就强行发送到用户邮箱中的任何电子邮件都可称作是垃圾邮件。垃圾邮件一般具有批量发送的特征，内容大多为广告信息、成人广告、商业或个人网站广告、电子杂志等不同的非正式信件。

为避免这些垃圾邮件，就必须要设置邮件过滤功能，要实现邮件过滤功能可以使用软件或硬件产品，不过硬件邮件过滤设备的价格比较让人难以接受，还需要技术支持费用，使用软件设置邮件过滤功能的成本则比较低，不过要靠工程师维护。下面介绍如何过滤垃圾邮件，设置黑白名单数据库，降低收到垃圾邮件的机率。

## 21.1 查询自己的邮件主机是否被当作垃圾邮件

如今使用电子邮件传递信息是最常用的通信手段，如果用户长时间大量发送邮件，其他邮件服务器很容易会把该邮件后缀列入垃圾邮件清单，不过不一定是大量发送邮件造成的，有可能是其他原因，如果被电子邮件服务器设置到黑名单中，用户往往不会知道。当用户收不到应该接收的邮件时，除了检查电子邮件服务器外，还要检查域名或IP地址是不是在垃圾邮件黑名单中。

查询垃圾邮件黑名单，所呈现的数据有可能不一样，有些数据库会是黑名单，有些却不是黑名单，原因在于黑名单数据库都是经过收集的，所以众多黑名单数据库不是每个都会被列入在内，不过若是查询很多黑名单数据库都是名列榜中，则域名或IP地址被当作黑名单的机率就特别高。

下面介绍三个常用的查询网址，特别推荐第三个What Is My IP Address，这里汇总了很多黑名单数据库，反垃圾邮件信息中心虽然数据少，但是已经足够各个公司使用，只要输入IP地址，经过查询就会出现测试结果，如果出来信息为已加入垃圾邮件，则代表你的域名或IP

地址已经列在黑名单之中，建议针对域名及IP地址都进行查询，因为有时查询结果不一样。

- MX Lookup Tool：http://www.mxtoolbox.com/index.aspx。

输入邮件域名，按【MX Lookup】即可以查询，所呈现的数据状态为红的话，代表已有数据库将该域名或IP地址列为黑名单。




- 反垃圾邮件信息中心：http://iscbl.anti-spam.cn/search.php。

此查询方式不能输入邮件域名，只能输入IP地址。




- What Is My IP Address - Check to see if your IP is on a blacklist。

http://whatismyipaddress.com/staticpages/index.php/is-my-ip-address-blacklisted
输入域名或IP地址，由于这个查询的数据库较多，所以速度会比较慢。




## 21.2 Postfix使用SpamAssassin过滤垃圾邮件

官方网站：http://spamassassin.apache.org/index.html。

SpamAssassin（SA）利用 Perl 来进行文字分析以达到过滤垃圾邮件的目的。它使用大量的默认规则检查信件，这些规则会检查发到内网所有邮件的标题、内文以及送信者。它采取的过滤方式是累加记分制，也就是说会根据我们所配置的标准来给予判定，当分数超过标准值的时候即判定为 SPAM（垃圾邮件）。2006年SpamAssassin被Linux新媒体奖（New Media Award）授予“最佳的基于Linux的反垃圾邮件解决方案”。

SpamAssassin使用多种方式检测垃圾邮件，包括垃圾邮件检测、邮件内容过滤、外部程序、黑名单和在线数据库等。

Postfix使用SpamAssassin（MTA）过滤垃圾邮件比使用Sendmail更方便配置，后面介绍的垃圾邮件及病毒信件配置都与此章节有关，若都要使用，由于有连贯性，建议确实做到每个步骤中的每个动作都不要略过，以免架设完成后有问题。

### 安装SpamAssassin软件

CentOS 6.x操作系统默认不会安装SpamAssassin服务软件，所以必须要自行安装，由于SpamAssassin服务涉及许多软件，建议使用YUM在线安装方式，以免手动安装有遗漏。

```
[root@localhost ~]# yum -y install spamassassin    //安装 SpamAssassin 软件
Dependencies Resolved
==========================================================================
 Package          Arch            Version                 Repository        Size
==========================================================================
Installing:
 spamassassin   x86_64        3.3.1-2.el6        base           1.1 M
```

```
Installing for dependencies:
 perl-Crypt-OpenSSL-Bignum   x86_64      0.04-8.1.el6    base34 k
 perl-Crypt-OpenSSL-RSA      x86_64      0.25-10.1.el6   base37 k
 perl-Crypt-OpenSSL-Random   x86_64      0.04-9.1.el6    base22 k
 perl-Digest-HMAC            noarch      1.01-22.el6     base22 k
 perl-Digest-SHA1            x86_64      2.12-2.el6      base49 k
 perl-Encode-Detect          x86_64      1.01-2.el6      base80 k
 perl-IO-Socket-INET6        noarch      2.56-4.el6      base17 k
 perl-IO-Socket-SSL          noarch      1.31-2.el6      base69 k
 perl-Mail-DKIM              noarch      0.37-2.el6      base121 k
 perl-MailTools              noarch      2.04-4.el6      base101 k
 perl-Net-DNS                x86_64      0.65-2.el6      base232 k
 perl-Net-LibIDN             x86_64      0.12-3.el6      base35 k
 perl-Net-SSLeay             x86_64      1.35-9.el6      base173 k
 perl-NetAddr-IP             x86_64      4.027-3.el6     base95 k
 perl-Socket6                x86_64      0.23-3.el6      base23 k
 perl-TimeDate               noarch      1:1.16-11.1.el6 base34 k
 portreserve                 x86_64      0.0.4-4.el6     base22 k
Transaction Summary
=========================================================================
Install      18 Package(s)
Upgrade       0 Package(s)
Total download size: 2.2 M
```

## 将Postfix配置为MTA

由于Postfix服务使用SpamAssassin功能，所以必须将Postfix邮件服务器配置为MTA，需要编辑Postfix服务的master.cf配置文件，此配置文件规定了Postfix服务运行参数，在配置文件内smtpd参数后面添加content_filter，使用SpamAssassin。

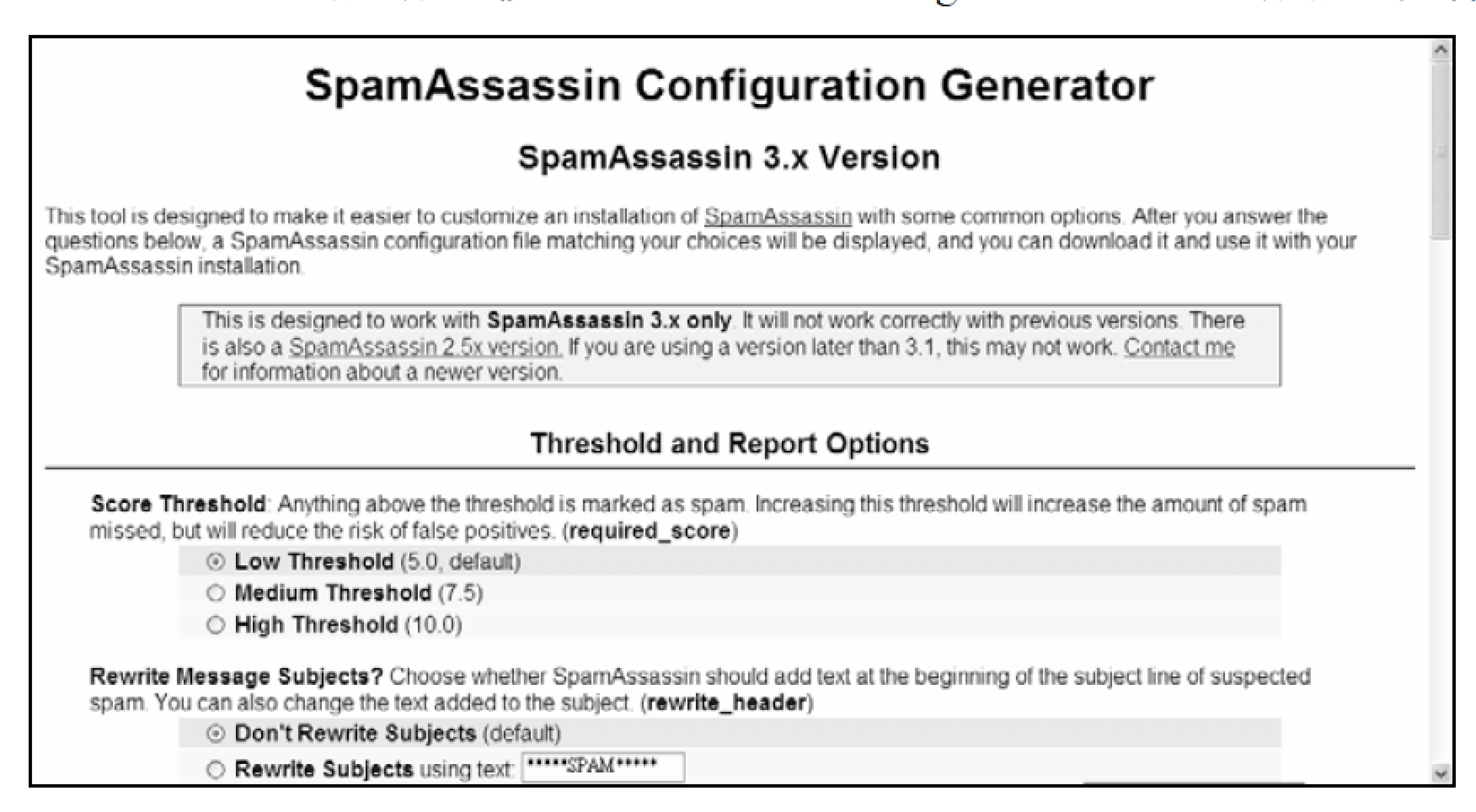
```
[root@localhost ~]# vi /etc/postfix/master.cf         //将 Postfix 配置为 MTA
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master").
#
# Do not forget to execute "postfix reload" after editing this file.
# =======================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# =======================================================================
smtp      inet  n       -       n       -       -       smtpd  -o content_filter=spamassassin
#submission inet n   -       n       -       -        smtpd
…中间省略…
spamassassin    unix    -    n    n    -  - pipe   user=nobody  argv=/usr/bin/spamc -f  -e
/usr/sbin/sendmail -oi -f ${sender} -- ${recipient}
                            //将上面的信息添加到文件的最后一行，此段为一行，不可以跳行
```

修改Postfix服务配置文件后，必须重新启动Postfix服务，配置才会生效。

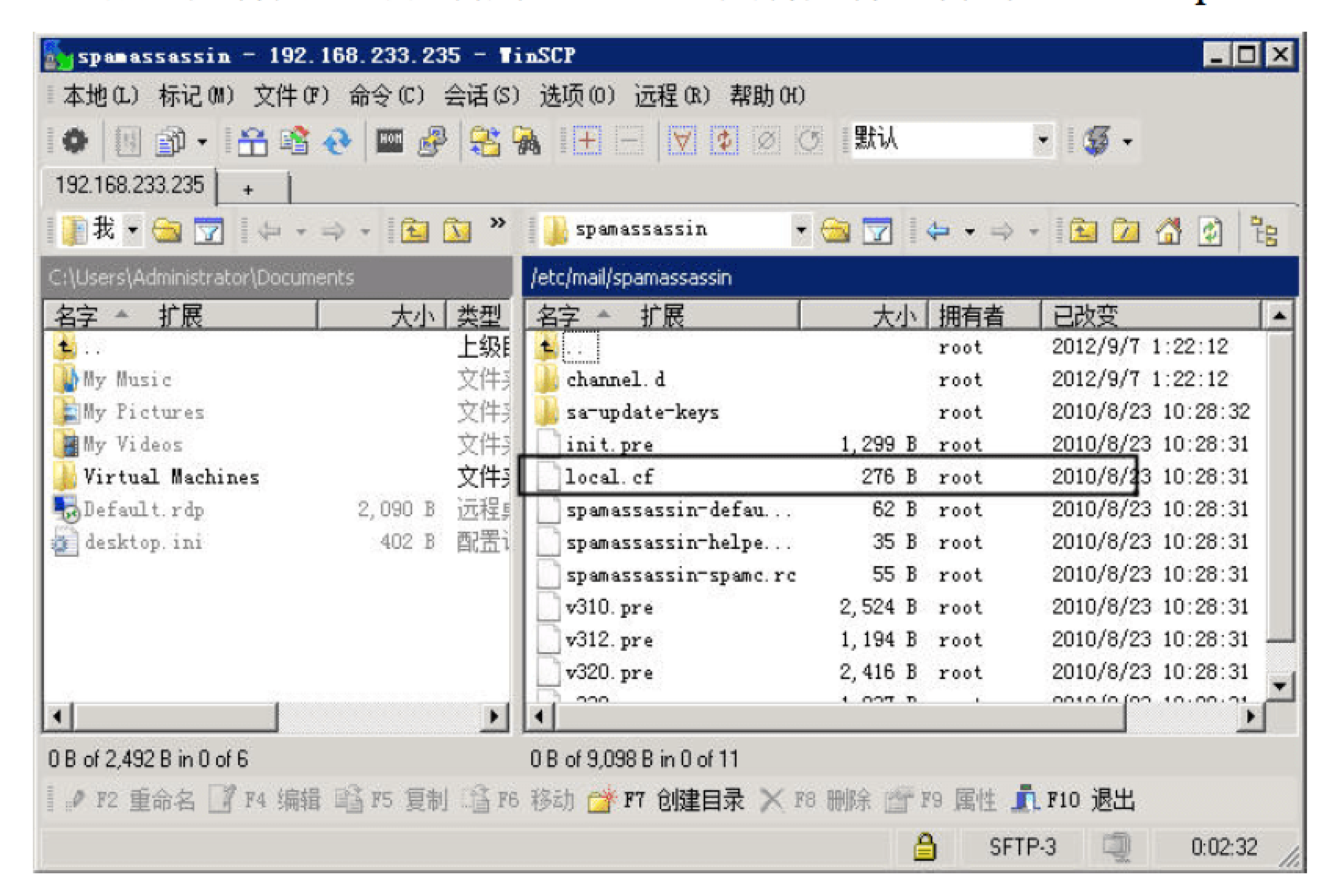
```
[root@localhost ~]# service postfix restart
Shutting down postfix:                                    [  OK  ]
Starting postfix:                                         [  OK  ]
```

## 生成SpamAssassin配置文件

SpamAssassin安装配置完成后，需要生成SpamAssassin服务的local.cf配置文件，local.cf配置文件是定义垃圾邮件的标准文件，此文件可以自行添加参数信息，如果不知道如何定义垃圾邮件标准，可以一律采用默认值，以后再根据运行情况修改标准。也可以到SpamAssassin Configuration Generator网站生成，按【Generate the Configuration File】生成配置文件。




生成local.cf配置文件后，可以利用WinSCP工具将文件上传到/etc/mail/spamassassin 目录。



说明

SpamAssassin Configuration Generator 3.X网站为http://www.yrex.com/spam/spamconfig.php。

SpamAssassin Configuration Generator 2.5X网站为http://www.yrex.com/spam/spamconfig25.php。

## 修改SpamAssassin配置文件

将local.cf配置文件上传至邮件服务器后，首先检查SpamAssassin配置文件的内容，由于刚刚生成local.cf文件，所以参数值都为默认，如果不了解参数的意义，切勿随意修改，以免信件被判定成垃圾邮件，导致用户无法收到信件。

```
[root@localhost ~]# vi /etc/mail/spamassassin/local.cf
# SpamAssassin config file for version 3.x
# NOTE: NOT COMPATIBLE WITH VERSIONS 2.5 or 2.6
# See http://www.yrex.com/spam/spamconfig25.php for earlier versions
# Generated by http://www.yrex.com/spam/spamconfig.php (version 1.50)
# How many hits before a message is considered spam.
required_score           5.0
# Encapsulate spam in an attachment (0=no, 1=yes, 2=safe)
report_safe             1
# Enable the Bayes system
use_bayes               1
# Enable Bayes auto-learning
bayes_auto_learn        1
# Enable or disable network checks
skip_rbl_checks         0
use_razor2              1
use_dcc                 1
use_pyzor               1
# Mail using languages used in these country codes will not be marked
# as being possibly spam in a foreign language.
ok_languages            all
# Mail using locales used in these country codes will not be marked
# as being possibly spam in a foreign language.
ok_locales              all
```

SpamAssassin服务配置文件的参数说明如下表。

| 参数 | 说明 |
| --- | --- |
| 分数线 required_score | 设定一个邮件被判定为垃圾邮件的分数线，默认为 5.0 分，分数越高，误判越低，分数越低，误判越高，依需求配置 |
| 识别邮件文件 report_safe | 默认为 1，当收到的信件被判定为垃圾邮件时，不修改原信件，而是创建一个新的报告信件，并且将原信件作为一个 RFC 822 格式的附件附上，建议设为 2，原信件以文本方式附加到报告信件中 |
| 使用 Bayesian 查询 use_bayes | 默认为 1 启动，0 为不启动，建议设为启动 |

（续表）

| 参数 | 说明 |
|---|---|
| 自动学习 bayes_auto_learn | 默认为 1 自动学习，0 为不学习，建议配置自动学习 |
| 使用 RBL 查询 skip_rbl_checks | 默认为 1 使用 RBLs 分析，0 为不学习 |
| 使用 razor 查询 use_razor2 | 默认为 1，必须安装 razor |
| 使用 dcc 查询 use_dcc | 默认为 1，必须安装 dcc |
| 使用 dccpyzor 查询 use_pyzor | 默认为 1，必须安装 dccpyzor |
| 语言设置 ok_languages、ok_locales | 默认为 all，接受所有语言 |

## 启动SpamAssassin 服务

SpamAssassin配置完成后，需要将SpamAssassin服务启动，由于SpamAssassin是搭配Postfix服务使用的，所以也将其设为系统默认启动

```
[root@localhost ~]# service spamassassin start//SpamAssassin 服务启动
Starting spamd:                                    [  OK  ]
[root@localhost ~]# chkconfig spamassassin on //SpamAssassinm 默认启动
```

## 测试SpamAssassin的功能

SpamAssassin正确启动后，首先测试它扫描垃圾邮件的能力，进入SpamAssassin模板文件目录，可以利用SpamAssassin服务的两个模板测试sample-nonspam.txt及sample-spam.txt，sample-spam.txt为垃圾邮件的模板，sample-nonspam.txt为非垃圾邮件模板。

```
[root@localhost ~]# cd /usr/share/doc/spamassassin*
                                    //进入 spamassassin 目录
[root@localhost spamassassin-3.3.1]#
```

说明

“*”号表示版本号，若您不知安装的是哪个版本就可以输入一个“*”号，让系统去识别。

首先测试垃圾邮件sample-spam.txt模板，SpamAssassin的local.cf配置文件默认分数值为5.0，超过此分数即判断为垃圾邮件，此模板内容垃圾邮件指数约为1000，经SpamAssassin检测，测试结果高达1000.0，说明判断垃圾邮件功能配置生效，SpamAssassin垃圾邮件处理能力也就没问题。

```
[root@localhost spamassassin-3.3.1]# spamassassin --test-mode  sample-spam.txt
Sep 20 19:54:50.879 [2000] warn: config: created user preferences file:
/root/.spamassassin/user_prefs
Received: from localhost by localhost.localdomain
        with SpamAssassin (version 3.3.1);
```

```
        Tue, 20 Sep 2011 19:54:52 -0400
From: Sender <sender@example.net>
To: Recipient <recipient@example.net>
Subject: Test spam mail (GTUBE)
Date: Wed, 23 Jul 2003 23:30:00 +0200
Message-Id: <GTUBE1.1010101@example.net>
X-Spam-Checker-Version: SpamAssassin 3.3.1 (2010-03-16) on
        localhost.localdomain
X-Spam-Flag: YES
X-Spam-Level: **************************************************
X-Spam-Status: Yes, score=1000.0 required=5.0 tests=GTUBE,NO_RECEIVED,
        NO_RELAYS autolearn=no version=3.3.1
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----------=_4E7927CC.6BE91BD9"
This is a multi-part message in MIME format.
------------=_4E7927CC.6BE91BD9
Content-Type: text/plain; charset=iso-8859-1
Content-Disposition: inline
Content-Transfer-Encoding: 8bit
Spam detection software, running on the system "localhost.localdomain", has
identified this incoming email as possible spam.  The original message
has been attached to this so you can view it (if it isn't spam) or label
similar future email.  If you have any questions, see
@@CONTACT_ADDRESS@@ for details.
Content preview:  This is the GTUBE, the Generic Test for Unsolicited Bulk Email
   If your spam filter supports it, the GTUBE provides a test by which you can
   verify that the filter is installed correctly and is detecting incoming spam.
   You can send yourself a test mail containing the following string of characters
   (in upper case and with no white spaces and line breaks): [...]
Content analysis details:   (1000.0 points, 5.0 required)
 pts rule name   description
------------------------------------------------------------------------
-0.0 NO_RELAYS   Informational: message was not relayed via SMTP
1000 GTUBE       BODY: Generic Test for Unsolicited Bulk Email
-0.0 NO_RECEIVED    Informational: message has no Received headers
------------=_4E7927CC.6BE91BD9
Content-Type: message/rfc822; x-spam-type=original
Content-Description: original message before SpamAssassin
Content-Disposition: inline
Content-Transfer-Encoding: 8bit
Subject: Test spam mail (GTUBE)
Message-ID: <GTUBE1.1010101@example.net>
Date: Wed, 23 Jul 2003 23:30:00 +0200
From: Sender <sender@example.net>
To: Recipient <recipient@example.net>
Precedence: junk
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
This is the GTUBE, the
```

```
        Generic
        Test for
        Unsolicited
        Bulk
        Email
If your spam filter supports it, the GTUBE provides a test by which you
can verify that the filter is installed correctly and is detecting incoming
spam. You can send yourself a test mail containing the following string of
characters (in upper case and with no white spaces and line breaks):
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
You should send this test mail from an account outside of your network.
------------=_4E7927CC.6BE91BD9--
Spam detection software, running on the system "localhost.localdomain", has
identified this incoming email as possible spam.  The original message
has been attached to this so you can view it (if it isn't spam) or label
similar future email.  If you have any questions, see
@@CONTACT_ADDRESS@@ for details.
Content preview:  This is the GTUBE, the Generic Test for Unsolicited Bulk Email
   If your spam filter supports it, the GTUBE provides a test by which you can
   verify that the filter is installed correctly and is detecting incoming spam.
   You can send yourself a test mail containing the following string of characters
   (in upper case and with no white spaces and line breaks): [...]
Content analysis details:   (1000.0 points, 5.0 required)
                                      //默认 5.0，分数超过 1000，判断为垃圾邮件
 pts rule name   description
------------------------------------------------------------------------
-0.0 NO_RELAYS   Informational: message was not relayed via SMTP
1000 GTUBE       BODY: Generic Test for Unsolicited Bulk Email
-0.0 NO_RECEIVED    Informational: message has no Received headers
```

其次测试非垃圾邮件sample-nonspam.txt模板，经SpamAssassin检测，此模板内容不符合垃圾邮件的条件，测试结果数值为0，代表SpamAssassin没有误判。以前的版本同一个模板检测出来数值不一定为0，虽然不会超过默认值5，但还是有可能被误判的。

```
[root@localhost spamassassin-3.3.1]# spamassassin --test-mode  sample-nonspam.txt
Return-Path: <tbtf-approval@world.std.com>
X-Spam-Checker-Version: SpamAssassin 3.3.1 (2010-03-16) on
        localhost.localdomain
X-Spam-Level:
X-Spam-Status: No, score=-0.0 required=5.0 tests=T_RP_MATCHES_RCVD
        autolearn=ham version=3.3.1
Delivered-To: foo@foo.com
Received: from europe.std.com (europe.std.com [199.172.62.20])
        by mail.netnoteinc.com (Postfix) with ESMTP id 392E1114061
        for <foo@foo.com>; Fri, 20 Apr 2001 21:34:46 +0000 (Eire)
Received: (from daemon@localhost)
        by europe.std.com (8.9.3/8.9.3) id RAA09630
        for tbtf-outgoing; Fri, 20 Apr 2001 17:31:18 -0400 (EDT)
Received: from sgi04-e.std.com (sgi04-e.std.com [199.172.62.134])
        by europe.std.com (8.9.3/8.9.3) with ESMTP id RAA08749
        for <tbtf@facteur.std.com>; Fri, 20 Apr 2001 17:24:31 -0400 (EDT)
```

```
Received: from world.std.com (world-f.std.com [199.172.62.5])
        by sgi04-e.std.com (8.9.3/8.9.3) with ESMTP id RAA8278330
        for <tbtf@facteur.std.com>; Fri, 20 Apr 2001 17:24:31 -0400 (EDT)
Received: (from dawson@localhost)
        by world.std.com (8.9.3/8.9.3) id RAA26781
        for tbtf@world.std.com; Fri, 20 Apr 2001 17:24:31 -0400 (EDT)
Received: from sgi04-e.std.com (sgi04-e.std.com [199.172.62.134])
        by europe.std.com (8.9.3/8.9.3) with ESMTP id RAA07541
        for <tbtf@facteur.std.com>; Fri, 20 Apr 2001 17:12:06 -0400 (EDT)
Received: from world.std.com (world-f.std.com [199.172.62.5])
        by sgi04-e.std.com (8.9.3/8.9.3) with ESMTP id RAA8416421
        for <tbtf@facteur.std.com>; Fri, 20 Apr 2001 17:12:06 -0400 (EDT)
Received: from [208.192.102.193] (ppp0c199.std.com [208.192.102.199])
        by world.std.com (8.9.3/8.9.3) with ESMTP id RAA14226
        for <tbtf@world.std.com>; Fri, 20 Apr 2001 17:12:04 -0400 (EDT)
Mime-Version: 1.0
Message-Id: <v0421010eb70653b14e06@[208.192.102.193]>
Date: Fri, 20 Apr 2001 16:59:58 -0400
To: tbtf@world.std.com
From: Keith Dawson <dawson@world.std.com>
Subject: TBTF ping for 2001-04-20: Reviving
Content-Type: text/plain; charset="us-ascii"
Sender: tbtf-approval@world.std.com
Precedence: list
Reply-To: tbtf-approval@europe.std.com
-----BEGIN PGP SIGNED MESSAGE-----
TBTF ping for 2001-04-20: Reviving
    T a s t y  B i t s f r o m  t h e  T e c h n o l o g y  F r o n t
    Timely news of the bellwethers in computer and communications
    technology that will affect electronic commerce -- since 1994
    Your Host: Keith Dawson
    ISSN: 1524-9948
    This issue: < http://tbtf.com/archive/2001-04-20.html >
    To comment on this issue, please use this forum at Quick Topic:
    < http://www.quicktopic.com/tbtf/H/kQGJR2TXL6H >
  _________________________________________________________________
Q u o t e   O f   T h e   M o m e n t
    Even organizations that promise "privacy for their customers" rarely
    if ever promise "continued privacy for their former customers..."
    Once you cancel your account with any business, their promises of
    keeping the information about their customers private no longer
    apply... you're not a customer any longer.
    This is in the large category of business behaviors that individuals
    would consider immoral and deceptive -- and businesses know are not
    illegal.
    -- "_ankh," writing on the XNStalk mailing list
_________________________________________________________________
..TBTF's long hiatus is drawing to a close
    Hail subscribers to the TBTF mailing list. Some 2,000 [1] of you
    have signed up since the last issue [2] was mailed on 2000-07-20.
    This brief note is the first of several I will send to this list to
    excise the dead addresses prior to resuming regular publication.
    While you time the contractions of the newsletter's rebirth, I in-
```

```
    vite you to read the TBTF Log [3] and sign up for its separate free
    subscription. Send "subscribe" (no quotes) with any subject to
    tbtf-log-request@tbtf.com . I mail out collected Log items on Sun-
    days.
    If you need to stay more immediately on top of breaking stories,
    pick up the TBTF Log's syndication file [4] or read an aggregator
    that does. Examples are Slashdot's Cheesy Portal [5], Userland [6],
    and Sitescooper [7]. If your news obsession runs even deeper and you
    own an SMS-capable cell phone or PDA, sign up on TBTF's WebWire-
    lessNow portal [8]. A free call will bring you the latest TBTF Log
    headline, Jargon Scout [9] find, or Siliconium [10].
    Two new columnists have bloomed on TBTF since last summer: Ted By-
    field's roving_reporter [11] and Gary Stock's UnBlinking [12]. Late-
    ly Byfield has been writing in unmatched depth about ICANN, but the
    roving_reporter nym's roots are in commentary at the intersection of
    technology and culture. Stock's UnBlinking latches onto topical sub-
    jects and pursues them to the ends of the Net. These writers' voices
    are compelling and utterly distinctive.
    [1]  http://tbtf.com/growth.html
    [2]  http://tbtf.com/archive/2000-07-20.html
    [3]  http://tbtf.com/blog/
    [4]  http://tbtf.com/tbtf.rdf
    [5]  http://www.slashdot.org/cheesyportal.shtml
    [6]  http://my.userland.com/
    [7]  http://www.sitescooper.org/
    [8]  http://tbtf.com/pull-wwn/
    [9]  http://tbtf.com/jargon-scout.html
    [10] http://tbtf.com/siliconia.html
    [11] http://tbtf.com/roving_reporter/
    [12] http://tbtf.com/unblinking/
__________________________________________________________________
S o u r c e s
> For a complete list of TBTF's email and Web sources, see
    http://tbtf.com/sources.html .
__________________________________________________________________
B e n e f a c t o r s
    TBTF is free. If you get value from this publication, please visit
    the TBTF Benefactors page < http://tbtf.com/the-benefactors.html >
    and consider contributing to its upkeep.
__________________________________________________________________
    TBTF home and archive at http://tbtf.com/ . To unsubscribe send
    the message "unsubscribe" to tbtf-request@tbtf.com. TBTF is Copy-
    right 1994-2000 by Keith Dawson, <dawson@world.std.com>. Commercial
    use prohibited. For non-commercial purposes please forward, post,
    and link as you see fit.
    _______________________________________________
    Keith Dawson              dawson@world.std.com
    Layer of ash separates morning and evening milk.
-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.5.2 for non-commercial use <http://www.pgp.com>
iQCVAwUBOuCi3WAMawgf2iXRAQHeAQQA3YSePSQ0XzdHZUVskFDkTfpE9XS4fHQs
WaT6a8qLZK9PdNcoz3zggM/Jnjdx6CJqNzxPEtxk9B2DoGll/C/60HWNPN+VujDu
Xav65S0P+Px4knaQcCIeCamQJ7uGcsw+CqMpNbxWYaTYmjAfkbKH1EuLC2VRwdmD
wQmwrDp70v8=
```

```
=8hLB
-----END PGP SIGNATURE-----
Spam detection software, running on the system "localhost.localdomain", has
identified this incoming email as possible spam.  The original message
has been attached to this so you can view it (if it isn't spam) or label
similar future email.  If you have any questions, see
@@CONTACT_ADDRESS@@ for details.
Content preview:  -----BEGIN PGP SIGNED MESSAGE----- TBTF ping for 2001-04-20:
   Reviving T a s t y B i t s f r o m t h e T e c h n o l o g y F r o n t [...]
Content analysis details:   (-0.0 points, 5.0 required)
                                            //默认 5，指数为 0，判定为非垃圾邮件
 pts rule name   description
-------------------------------------------------------------------------
-0.0 T_RP_MATCHES_RCVD Envelope sender domain matches handover relay
                          domain
```

## 实际测试垃圾邮件

SpamAssassin模板测试完成后，并不一定代表实际环境SpamAssassin功能没问题，这样只能看出SpamAssassin功能是否正常运行，无法看出SpamAssassin服务是否对邮件真的有过滤作用，接下来实际发送邮件测试，看SpamAssassin是否能正常过滤邮件。

例如，使用两个电子邮件账号jerry及tom，由jerry发送邮件给tom，发送一封垃圾邮件与一封正常邮件，测试是否会正确判别垃圾邮件及正常邮件，范例邮件内容数据如下表所示。

| | |
|---|---|
| **发件人** | jerry@jerryit.idv.cn |
| **收件者** | tom@jerryit.idv.cn |
| **垃圾邮件主题** | 垃圾邮件测试 |
| **正常邮件主题** | 正常邮件测试 |
| **垃圾邮件内容** | XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X |
| **正常邮件内容** | Test |

> **说明**
> 垃圾邮件内容可以在SpamAssassin的sample-spam.txt模板中找到。

首先发送垃圾邮件测试，使用jerry账号发送垃圾邮件给tom，输入垃圾邮件内容，然后发送邮件。

发送人： "jerry" <jerry@jerryit.idv.cn> 优先： 普通
收信人： tom@jerryit.idv.cn
抄送：
秘密抄送：
回信给： 要求读取回条
附件： 浏览... 添加
主题： 垃圾邮件测试 保存发件备份
寄信 保存草稿 拼字检查 english 信件格式： 纯文本 取消
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
--
Open WebMail Project(http://openwebmail.org)

检查邮件日志文件，发现该邮件分数到达999.0分，被SpamAssassin服务判断为垃圾邮件。

```
[root@mail ~]# cat /var/log/maillog
Sep 20 22:28:27 localhost spamd[3855]: spamd: processing message
<20110921022730.M9951@jerrit.idv.cn> for nobody:99
Sep 20 22:28:28 localhost spamd[3855]: spamd: identified spam(999.0/5.0)
for nobody:99 in .4 seconds, 605 bytes.
Sep 20 22:28:28 localhost spamd[3855]: spamd:
result: Y 999 - ALL_TRUSTED,GTUBE
scantime=0.,size=605,user=nobody,uid=99,required_score=5.0,rhost=localhost,
raddr=127.0.0.1,rport=55647mid=<20120921022730.M9951@jerryit.idv.cn>,
autolearn=no
```

接下来发送正常邮件测试，使用jerry账号发送正常邮件给tom，输入正常邮件内容，然后发送邮件。




检查邮件日志文件，发现检测结果只有-1.0，说明信件内容未达垃圾邮件标准，SpamAssassin服务判断为正常邮件。

```
[root@mail ~]# cat /var/log/maillog
Sep 20 22:31:09 localhost spamd[3855]: plugin: eval failed: bayes:(in learn) locker:
safe_lock: cannot create tmp lockfile
/.spamassassin/bayes.lock.mail.jerryit.idv.cn.3855 for /.spamassassin/bayes.lock:
No such file or directory
Sep 20 22:31:09 localhost spamd[3855]: spamd: clean message(-1.0/5.0) for
nobody:99 in 0.2 seconds, 542 bytes.
Sep 20 22:31:09 localhost spamd[3855]: spamd: result: . -1 - ALL_TRUSTED
scantime=0.2,size=542,user=nobody,uid=99,required_score=5.0,rhost=localhost,
```

```
raddr=127.0.0.1,rport=49174,mid=<20120921023041.M99843@jerryit.idv.cn>,
autolearn=unavailable
```

根据以上邮件日志信息，可以确定SpamAssassin服务已正确判断出邮件的性质，到这一步算是成功了三分之一，再用tom账号登录邮箱，OpenWebMail就会弹出提示窗口，如下图所示。




关闭弹出的提示窗口，进入收件箱，可以看到一封主题为正常邮件测试的邮件，如下图所示。




那再进入广告邮件，可以看到一封主题为垃圾邮件测试的邮件，这就代表SpamAssassin服务能够百分百检测到垃圾邮件。




# 21.3 让SpamAssassin增加检测垃圾邮件功能

SpamAssassin服务虽然有不错的垃圾邮件判断能力，但毕竟不是万能的，原因是SpamAssassin不会马上将信件归为垃圾邮件，等SpamAssassin收集到一定数量的模板时，SpamAssassin才会将其归为垃圾邮件。SpamAssassin在默认情况下，通过贝叶斯过滤以加强spam的规则，通过用户输入命令来实现贝叶斯学习是最有效的方法。为此SpamAssassin 服务提供命令行工具sa-learn，让SpamAssassin服务识别用户收到的各种不同的垃圾邮件。

## 建立SpamAssassin学习账号

在配置SpamAssassin自动学习垃圾邮件能力之前，必须先建立两个邮件账号，账号名称分

别为spammail及nospammail。

| 账号名称 | 账号功能 |
| --- | --- |
| spammail | 负责让 spamassassin 学习未被归为垃圾邮件的信箱 |
| nospammail | 负责让 spamassassin 学习误判为垃圾邮件的信箱 |

## 学习垃圾邮件命令

在/var/spool/mail/目录中创建spammail为垃圾邮件账号的邮件目录，命令格式如下：

```
[root@mail ~]# /usr/bin/sa-learn  --showdots  --spam  --mbox  /var/spool/mail/spammail
Learned tokens from 0 message (s) (0 message (s) examined)
```

## 学习非垃圾邮件命令

在/var/spool/mail/目录中创建nospammail为非垃圾邮件账号的邮件目录，命令格式如下：

```
[root@mail ~]# /usr/bin/sa-learn  --showdots   --ham  /var/spool/mail/nospammail
Learned tokens from 0 message (s) (0 message (s) examined)
```

## 检查目前学习状况

所有信件都是SpamAssassin的学习模板，SpamAssassin不会马上将信件归为垃圾邮件，等SpamAssassin收集到一定数量的模板时，SpamAssassin才会将其归类为垃圾邮件，要归类成垃圾邮件需要的模板也要高达一两百封。

```
[root@mail ~]# sa-learn --dump magic
0.000          0          3          0  non-token data: bayes db version
0.000          0          0          0  non-token data: nspam
0.000          0          1          0  non-token data: nham
0.000          0        487          0  non-token data: ntokens
0.000          0  987802486          0  non-token data: oldest atime
0.000          0  987802486          0  non-token data: newest atime
0.000          0          0          0  non-token data: last journal sync atime
0.000          0          0          0  non-token data: last expiry atime
0.000          0          0          0  non-token data: last expire atime delta
0.000          0          0          0  non-token data: last expire reduction count
```

如果要SpamAssassin重新学习，可以输入【sa-learn--clear】，模板统计数量就会重新收集计算。

## 使用计划任务实现自动学习

要让SpamAssassin每天都学习新的垃圾邮件模板，建议将学习命令加入到计划任务中，这

样每天可自动从信箱内收集模板数量。

```
* 1,13 * * * /usr/bin/sa-learn --showdots --spam --mbox /var/spool/mail/spammail
* 1,13 * * *  /usr/bin/sa-learn --showdots --ham --mbox /var/spool/mail/nospammail
```

# 21.4 手动配置黑白名单

SpamAssassin服务可以自动学习垃圾邮件，不过要在收集模板数量并分析后才会归类为垃圾邮件，这样的速度太慢了！有一个快速的方式，就是直接将域名配置为黑名单，将禁止的名单配置到黑名单中，配置完毕后，用户就不会收到该垃圾邮件了，既然有黑名单，也就有白名单，配置白名单是以防SpamAssassin服务误判，配置白名单后，SpamAssassin服务就不会判为垃圾邮件，配置方式就是修改垃圾邮件标准定义文件local.cf。

## 配置黑白名单

例如，将后缀为jerryit.idv.cn的所有账号都配置为黑名单，但特定jerry账号为白名单，如下表所示。

| | |
|---|---|
| **单一用户账号** | jerry@jerryit.idv.cn |
| **网内所有用户账号** | *@jerryit.idv.cn |

- 黑名单blacklist_from参数配置将域名为jerryit.idv.cn的所有邮件都列为黑名单，无法收到信件。
- 白名单whitelist_from参数配置可以收到jerry@jerryit.idv.cn发送的邮件。

配置条件模板，编辑垃圾邮件标准定义文件，将黑名单配置为该域名内的所有账号，白名单配置为jerry账号。

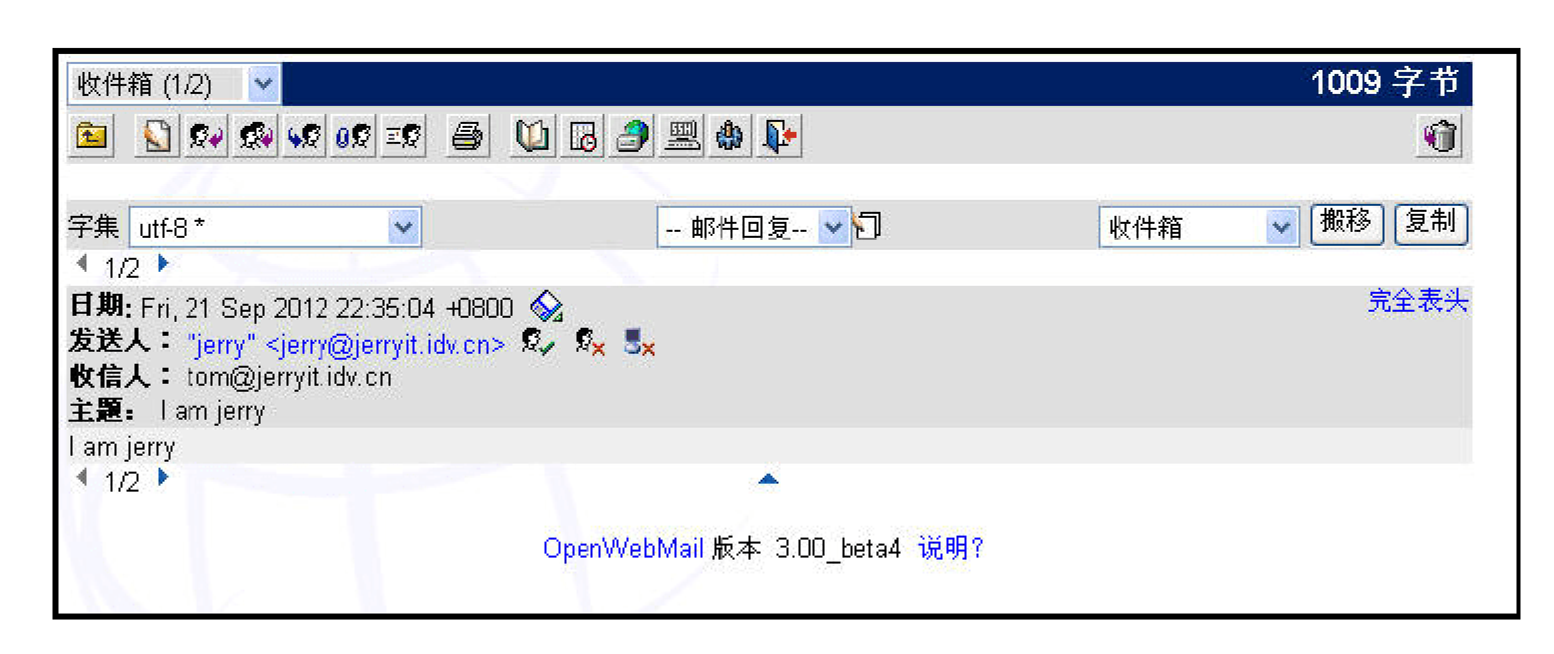
```
[root@mail ~]# vi /etc/mail/spamassassin/local.cf
blacklist_from  *@jerryit.idv.cn          //黑名单
whitelist_from  jerry@jerryit.idv.cn      //白名单
```

黑白名单配置完毕后，必须重新启动SpamAssassin服务，配置才会生效。

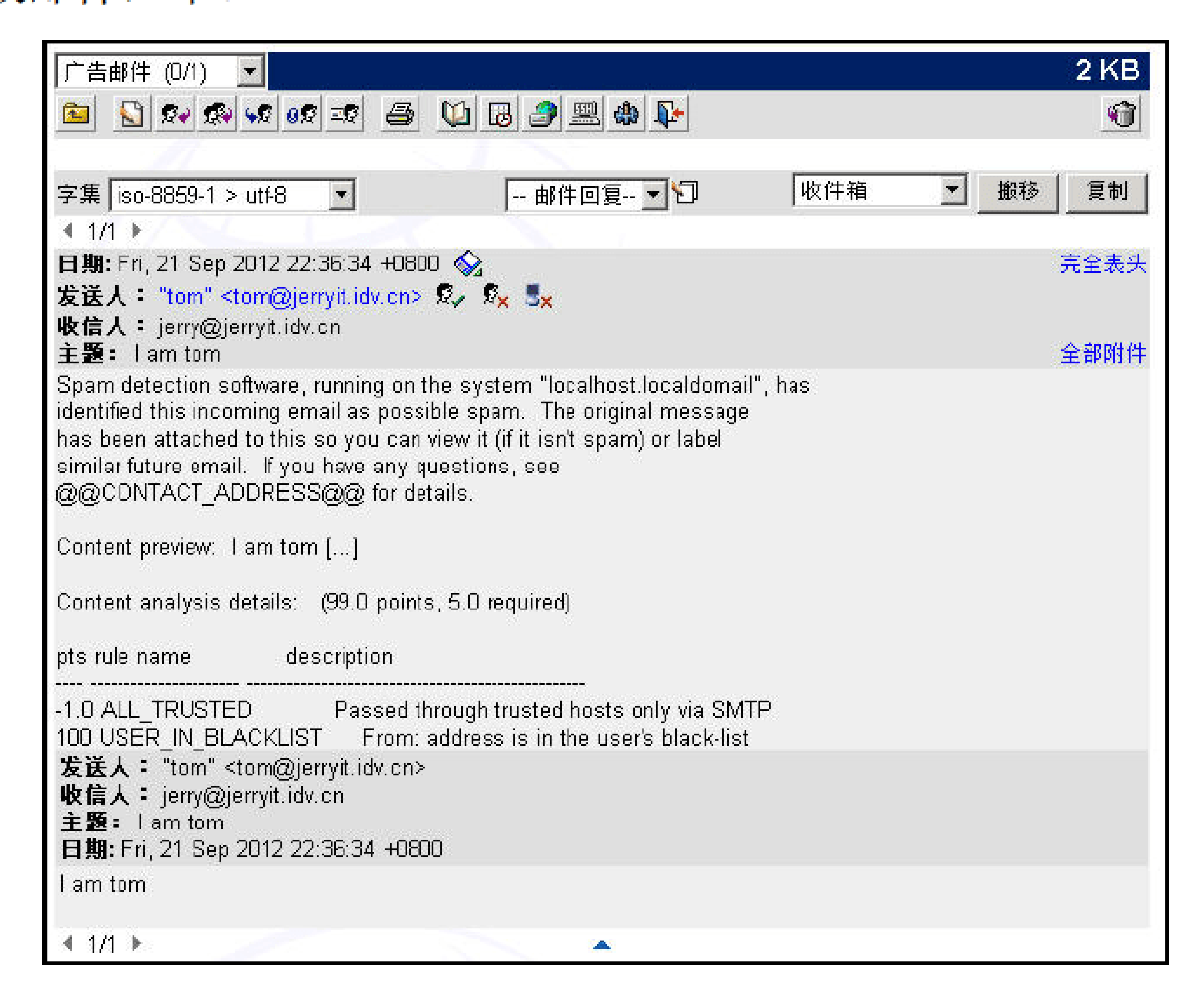
```
[root@mail ~]# service spamassassin restart
Stopping spamd:                  [  OK  ]
Starting spamd:                  [  OK  ]
```

## 测试SpamAssassin黑白名单

首先测试白名单，使用jerry账号发送邮件给tom，检查新邮件的邮件内容是否有警告信息，如下图所示。邮件内容可以正常查看，没有警告信息。




其次测试黑名单，使用tom账号发送邮件给jerry，看看可不可以在收件箱中收到邮件，如果收件箱中没有的话，可能在广告邮件中，而且有SPAM提示信息，如下图所示，邮件被归类到广告邮件（垃圾邮件）中。



# 第22章

# Virus——过滤病毒邮件

如今电子邮件被广泛使用，计算机病毒往往会藏于电子邮件中，导致用户通过电子邮件而中毒，所以对邮件服务器安装防病毒软件是有必要的，下面介绍MailScanner、Clamav的使用。

## 22.1 MailScanner电子邮件安全系统

MailScanner官方网站：http://www.mailscanner.info/。

MailScanner是一套电子邮件安全系统，可以使用扫毒软件（Clamv）及广告信息判断引擎（SpamAssassin）来增加其过滤功能。它同时具有邮件过滤的功能。

### 安装必备软件

安装MailScanner服务，需要许多必备软件，必备软件数量很多，务必都要安装，不要缺少任何一个软件，可由yum在线更新方式进行快速安装。

```
[root@localhost ~]# yum -y install rpm-build gcc-c++ rpm-devel zlib-devel libstdc++-devel
bzip2-devel docbook-utils beecrypt-devel elfutils-devel gettext ncurses-devel
readline-devel libselinux-devel
Dependencies Resolved
=======================================================================
 Package                Arch      Version                 Repository      Size
=======================================================================
Installing:
 bzip2-devel          x86_64    1.0.5-7.el6_0          updates        250 k
 docbook-utils        noarch    0.6.14-24.el6          base            69 k
 elfutils-devel       x86_64    0.148-1.el6            base            66 k
 gcc-c++              x86_64    4.4.4-13.el6           base           4.7 M
 libselinux-devel     x86_64    2.0.94-2.el6           base           135 k
 libstdc++-devel      x86_64    4.4.4-13.el6           base           1.5 M
 ncurses-devel        x86_64    5.7-3.20090208.el6     base           642 k
 readline-devel       x86_64    6.0-3.el6              base           134 k
 rpm-build            x86_64    4.8.0-12.el6           base           122 k
 rpm-devel            x86_64    4.8.0-12.el6           base            88 k
```

```
 zlib-devel            x86_64   1.2.3-25.el6          base           43 k
Installing for dependencies:
 docbook-dtds          noarch    1.0-51.el6           base          274 k
 docbook-style-dsssl   noarch    1.79-10.el6          base          277 k
 elfutils-libelf-devel x86_64    0.148-1.el6          base           30 k
 file-devel            x86_64    5.04-6.el6           updates        23 k
 libsepol-devel        x86_64    2.0.41-3.el6         base           64 k
 openjade              x86_64    1.3.2-36.el6         base          817 k
 opensp                x86_64    1.5.2-12.1.el6       base          872 k
 perl-SGMLSpm          noarch    1.03ii-21.el6        base           26 k
 popt-devel            x86_64    1.13-7.el6           base           21 k
 sgml-common           noarch    0.6.3-32.el6         base           43 k
 xml-common            noarch    0.6.3-32.el6         base          9.5 k
Updating for dependencies:
 bzip2-libs            x86_64    1.0.5-7.el6_0        updates        36 k
 file                  x86_64    5.04-6.el6           updates        44 k
 file-libs             x86_64    5.04-6.el6           updates       309 k
Transaction Summary
========================================================================
Install      22 Package(s)
Upgrade       3 Package(s)
Total download size: 11 M
```

## 下载并解压MailScanner软件

MailScanner 安装文件为压缩文件，可以从官方网站使用 wget 命令下载，然后解压缩。

```
[root@localhost ~]# wget
http://www.mailscanner.info/files/4/rpm/MailScanner-4.84.3-1.rpm.tar.gz
[root@localhost ~]# tar -zxvf MailScanner-4.84.3-1.rpm.tar.gz
```

> 说明
>
> MailScanner下载页面：http://www.mailscanner.info/downloads.html。

## 安装MailScanner 软件

解压缩后，进入MailScanner安装目录，按官方说明安装MailScanner，安装时间大约10分钟，如果没有安装必备软件，则安装过程中会发生错误，无法安装。

```
[root@localhost ~]# cd MailScanner*      //进入 MailScanner 安装目录[root@localhost
MailScanner-4.84.3-1]# ./install.sh
                                         //安装 MailScanner
…中间省略…
----------------------------------------------------------
Please buy the MailScanner book from www.mailscanner.info!
It is a very useful administration guide and introduction
to MailScanner. All the proceeds go directly to making
MailScanner a better supported package than it is today.
```

MailScanner可以与Sendmail或Postfix搭配使用，下面只介绍在Postfix环境中使用MailScanner，毕竟CentOS 6.x默认已经不使用Sendmail服务了。

## 配置Postfix使用MailScanner

编辑Postfix配置文件，将header_checks前面的【#】号删除，开启Postfix的header_checks参数。

```
[root@localhost ~]# vi /etc/postfix/main.cf
# The header_checks parameter specifies an optional table with patterns
# that each logical message header is matched against, including
# headers that span multiple physical lines.
#
# By default, these patterns also apply to MIME headers and to the
# headers of attached messages. With older Postfix versions, MIME and
# attached message headers were treated as body text.
#
# For details, see "man header_checks".
#
header_checks = regexp:/etc/postfix/header_checks    //删除#号，配置才会生效
```

在Postfix配置文件中开启header_checks后，再修改header_checks文件，添加【/^Received:/ HOLD】，这一行一定要加在最前面，否则配置不会生效。

```
[root@localhost ~]# vi /etc/postfix/header_checks
/^Received:/ HOLD          //将所收到的信先暂存在/var/spool/postfix/hold 目录
# HEADER_CHECKS (5)                                              HEADER_CHECKS (5)
#
```

**说明**

【/】后面的符号输入方式为Shift+6。

## 检查MailScanner使用的用户与用户组

检查目前用户、用户组及队列目录：

```
[root@localhost ~]# postconf |grep -E 'mail_owner|setgid_group|queue_directory'
mail_owner = postfix                  //执行 Postfix 用户
queue_directory = /var/spool/postfix  //Postfix 队列目录
setgid_group = postdrop               //执行 Postfix 用户组
```

检查结果内容如下。

| | |
|---|---|
| mail_owner 用户 | postfix |
| setgid_group 用户组 | postdrop |
| 收信队列目录 | /var/spool/postfix/hold |
| 发信队列目录 | /var/spool/postfix/incoming |

## 配置MailScanner

编辑MailScanner配置文件，Run As User用户名称输入Postfix用户，Run As Group用户组输入Postfix用户组名称postdrop。

```
[root@localhost ~]# vi /etc/MailScanner/MailScanner.conf
# User to run as (not normally used for sendmail)
# If you want to change the ownership or permissions of the quarantine or
# temporary files created by MailScanner, please see the "Incoming Work"
# settings later in this file.
#Run As User = mail
#Run As User = postfix
Run As User = postfix          //配置 Postfix 用户名称
# Group to run as (not normally used for sendmail)
#Run As Group = mail
#Run As Group = postfix
Run As Group = postdrop          //配置 Postfix 用户组名称
```

Postfix用户及用户组配置完成后，接下来配置Postfix发送和接收邮件的队列目录，Postfix队列目录名称分别为hold及incoming，如果邮件服务器有队列邮件，则会出现在这两个目录内。

```
[root@localhost ~]# vi /etc/MailScanner/MailScanner.conf
…中间省略…
#
#Incoming Queue Dir = /var/spool/mqueue.in
Incoming Queue Dir = /var/spool/postfix/hold  //Postfix 接收邮件的队列目录
# Set location of outgoing mail queue.
# This can also be the filename of a ruleset.
#Outgoing Queue Dir = /var/spool/mqueue
Outgoing Queue Dir = /var/spool/postfix/incoming
                                         //Postfix 发送邮件的队列目录
```

MailScanner 默认的MTA为Sendmail搭配MailScanner，现在要使用Postfix搭配MailScanner，所以要配置为postfix。

```
[root@localhost ~]# vi /etc/MailScanner/MailScanner.conf
# Set whether to use postfix, sendmail, exim or zmailer.
# If you are using postfix, then see the "SpamAssassin User State Dir"
# setting near the end of this file
MTA = postfix                              //默认为 Sendmail，修改为 Postfix
```

## 将hold及incoming配置为用户及用户组

上述MailScanner配置Postfix发送接收的队列目录，所以必须将Postfix的hold及incoming两个队列目录配置为Postfix的用户及用户组。

```
[root@localhost ~]# chown postfix.postdrop  /var/spool/MailScanner/incoming
                                    //配置 Postfix 接收队列目录的用户与用户组
[root@localhost ~]# chown postfix.postdrop /var/spool/MailScanner/quarantine
```

```
                                              //配置 Postfix 发送队列目录的用户与用户组
```

## 启动MailScanner

一切配置完成后，先将Postfix服务停用，原因在于MailScanner服务启动时会一并将Postfix服务启动，如果Postfix服务启动，再启动MailScanner服务，就会提示错误信息，所以在MailScanner启动前必须要停用Postfix服务。

从CentOS 6.x版本开始，Postfix为默认启动的服务，所以也要将Postfix服务设为默认不启动，然后将MailScanner服务设为默认启动，在每次重新启动时，Postfix才不会重复启动。

```
[root@localhost ~]# service postfix stop    //停用 Postfix 服务
Shutting down postfix:                        [  OK  ]
[root@localhost ~]# chkconfig postfix off     //Postfix 服务设为默认停用
[root@localhost ~]# chkconfig MailScanner on  //MailScanner 设为默认启动
[root@localhost ~]# service MailScanner start //启动 MailScanner 服务
Starting MailScanner daemons:
        incoming postfix:                     [  OK  ]
        outgoing postfix:                     [  OK  ]
        MailScanner:                          [  OK  ]
```

如果启动后无法收到邮件，检查一下/var/log/maillog日志文件，发现Could not create Processing Attempts Database信息，此错误信息在CentOS 6.x版本中才会出现。

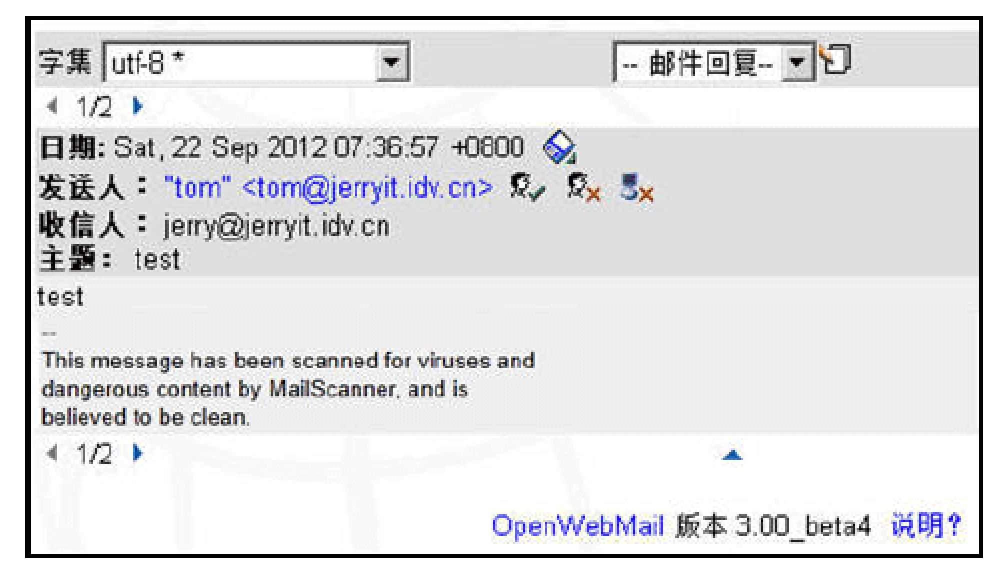
```
[root@localhost ~]# vi /var/log/maillog
Sep 21 20:25:36 localhost MailScanner[7881]: Could not create Processing Attempts Database
"/var/spool/MailScanner/incoming/Processing.db"
Sep 21 20:25:36 localhost MailScanner[7881]: Using locktype = flock
```

原因在于incoming目录内的Processing.db文件，需要配置Postfix用户与用户组，所以需要为Processing.db配置Postfix用户与用户组，邮件即可以正常发送。

```
[root@localhost postfix]# cd /var/spool/MailScanner/incoming
[root@localhost incoming]# chown postfix.postdrop Processing.db
```

## 测试MailScanner

MailScanner服务正常启动后，利用tom用户给jerry用户发送邮件，如果邮件内容出现MailScanner扫描的信息，如下图所示，代表MailScanner服务与Postfix服务配置成功。



## 22.2 SpamAssassin + MailScanner

如果要让Postfix服务搭配使用SpamAssassin及 MailScanner服务，需要对SpamAssassin邮件过滤服务及 MailScanner邮件扫描服务进行配置，首先需要对MailScanner服务进行配置，这样才可以和SpamAssassin一起使用，邮件服务器就可以起到邮件过滤和邮件扫描的作用。

### 配置MailScanner使用SpamAssassin

编辑MailScanner配置文件，配置MailScanner的SpamAssassin User State Dir目录路径。

```
[root@localhost ~]# vi /etc/MailScanner/MailScanner.conf
# The per-user files (bayes, auto-whitelist, user_prefs) are looked
# for here and in ~/.spamassassin/. Note the files are mutable.
# If this is unset then no extra places are searched for.
# If using Postfix, you probably want to set this as shown in the example
# line at the end of this comment, and do
#      mkdir /var/spool/MailScanner/spamassassin
#      chown postfix.postfix /var/spool/MailScanner/spamassassin
# NOTE: SpamAssassin is always called from MailScanner as the same user,
#       and that is the "Run As" user specified above. So you can only
#       have 1 set of "per-user" files, it's just that you might possibly
#       need to modify this location.
#       You should not normally need to set this at all.
#SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin
SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin
```

接下来配置SpamAssassin Site Rules Dir目录路径，如果前面有【#】号需要删除，才可以使用。

```
[root@localhost ~]# vi /etc/MailScanner/MailScanner.conf
# The site rules are searched for here.
# Normal location on most systems is /etc/mail/spamassassin.
SpamAssassin Site Rules Dir = /etc/mail/spamassassin
```

MailScanner配置文件配置完成后，必须创建MailScanner的SpamAssassin User State Dir目录，默认MailScanner目录下没有Spamassassin目录，所以必须自行创建，然后修改为Postfix用户及用户组权限。

```
[root@localhost ~]# mkdir -p /var/spool/MailScanner/spamassassin
[root@localhost ~]# chown postfix.postdrop /var/spool/MailScanner/spamassassin
```

### 配置MailScanner关闭Spam Checks

编辑MailScanner 配置文件，修改Spam Checks参数，默认为yes，修改为no。

```
[root@localhost ~]# vi /etc/MailScanner/MailScanner.conf
# Do you want to check messages to see if they are spam?
```

```
# Note: If you switch this off then *no* spam checks will be done at all.
#       This includes both MailScanner's own checks and SpamAssassin.
#       If you want to just disable the "Spam List" feature then set
#       "Spam List =" (i.e. an empty list) in the setting below.
# This can also be the filename of a ruleset.
Spam Checks = no                //默认为 yes，邮件会直接被 MailScanner 删除
```

说明

MailScanner配置文件必须将Spam Checks设为no，如果不设为no，SpamAssassin 及MailScanner服务搭配使用时，检测到的垃圾邮件都会被MailScanner服务直接删除，日志文件内容如下。

```
Sep 22 22:27:23 localhost MailScanner[13963]: Spam Checks: Found 1 spam messages
Sep 22 22:27:23 localhost MailScanner[13963]: Deleted 1 messages from
processing-database
```

## 重新启动SpamAssassin 及 MailScanner

虽然SpamAssassin服务没有修改配置文件，但为了让MailScanner 能够更好地搭配SpamAssassin服务，需要重新启动SpamAssassin服务，然后再重新启动MailScanner服务。

```
[root@localhost ~]# service spamassassin restart
Stopping spamd:                                            [  OK  ]
Starting spamd:                                            [  OK  ]
```

SpamAssassin服务重新启动完成后，再将MailScanner服务重新启动。

```
[root@localhost ~]# service MailScanner restart
Shutting down MailScanner daemons:
         MailScanner:                                      [  OK  ]
         incoming postfix:                                 [  OK  ]
         outgoing postfix:                                 [  OK  ]
Waiting for MailScanner to die gracefully ... dead.
Starting MailScanner daemons:
         incoming postfix:                                 [  OK  ]
         outgoing postfix:                                 [  OK  ]
         MailScanner:                                      [  OK  ]
```

## 测试SpamAssassin 及 MailScanner服务搭配使用

使用tom账户发送垃圾邮件给jerry账户，查看结果是否被删除，还是被分类为垃圾邮件。垃圾邮件的内容如下。

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```




邮件发送后，检查邮件传送日志，在日志文件内可以看到邮件垃圾邮件指数为999.0，所以将其判定为垃圾邮件，在日志文件内也可以看到MailScanner运行的记录。

```
[root@localhost ~]# cat /var/log/maillog
Sep 21 21:54:20 localhost MailScanner[13686]:
New Batch:Scanning 1 messages, 1195 bytes
Sep 21 21:54:20 localhost MailScanner[13686]:
Virus and Content Scanning: Starting
Sep 21 21:54:21 localhost MailScanner[13686]:
Requeue: 57F98C24A4.A2D0E to D2FB5C24A9
Sep 21 21:54:21 localhost postfix/qmgr[13585]:
D2FB5C24A9: from=<tom@jerryit.idv.cn>, size=576, nrcpt=1 (queue active)
Sep 21 21:54:21 localhost MailScanner[13686]:
Uninfected: Delivered 1 messages
Sep 21 21:54:21 localhost spamd[13402]:
spamd: connection from localhost [127.0.0.1] at port 52600
Sep 21 21:54:21 localhost spamd[13402]:
spamd: setuid to nobody succeeded
Sep 21 21:54:21 localhost spamd[13402]:
spamd: creating default_prefs: //.spamassassin/user_prefs
Sep 21 21:54:21 localhost MailScanner[13686]:
Deleted 1 messages from processing-database
Sep 21 21:54:21 localhost spamd[13402]:
config: cannot create user preferences file //.
spamassassin/user_prefs: No such file or directory
Sep 21 21:54:21 localhost spamd[13402]:
spamd: failed to create readable default_prefs: //.spamassassin/user_prefs
Sep 21 21:54:21 localhost spamd[13402]:
spamd: processing message 20120922015349.M46585@jerryit.idv.cnfor nobody:99
Sep 21 21:54:21 localhost spamd[13402]:
spamd:identified spam (999.0/5.0) for nobody:99 in 0.3 seconds, 909 bytes.
Sep 21 21:54:21 localhost spamd[13402]:
spamd: result: Y 999 - ALL_TRUSTED,
GTUBE scantime=0.3,size=909,user=nobody,uid=99,
required_score=5.0,rhost=localhost,raddr=127.0.0.1,rport=52600,mid=<20110922015349.M4
6585@jerryit.idv.cn>,autolearn=no
```

邮件测试中发现可以收到正常邮件，但是垃圾邮件则会被自动删除，查看邮件日志文件时出现以下信息，发生原因不明，以前CentOS 5.x不会有这样的问题，解决的方法是将Spam Checks这个配置值由no改回yes后，再次重新启动服务，再将yes改成no，再次重新启动服务后，问题就可以排除。

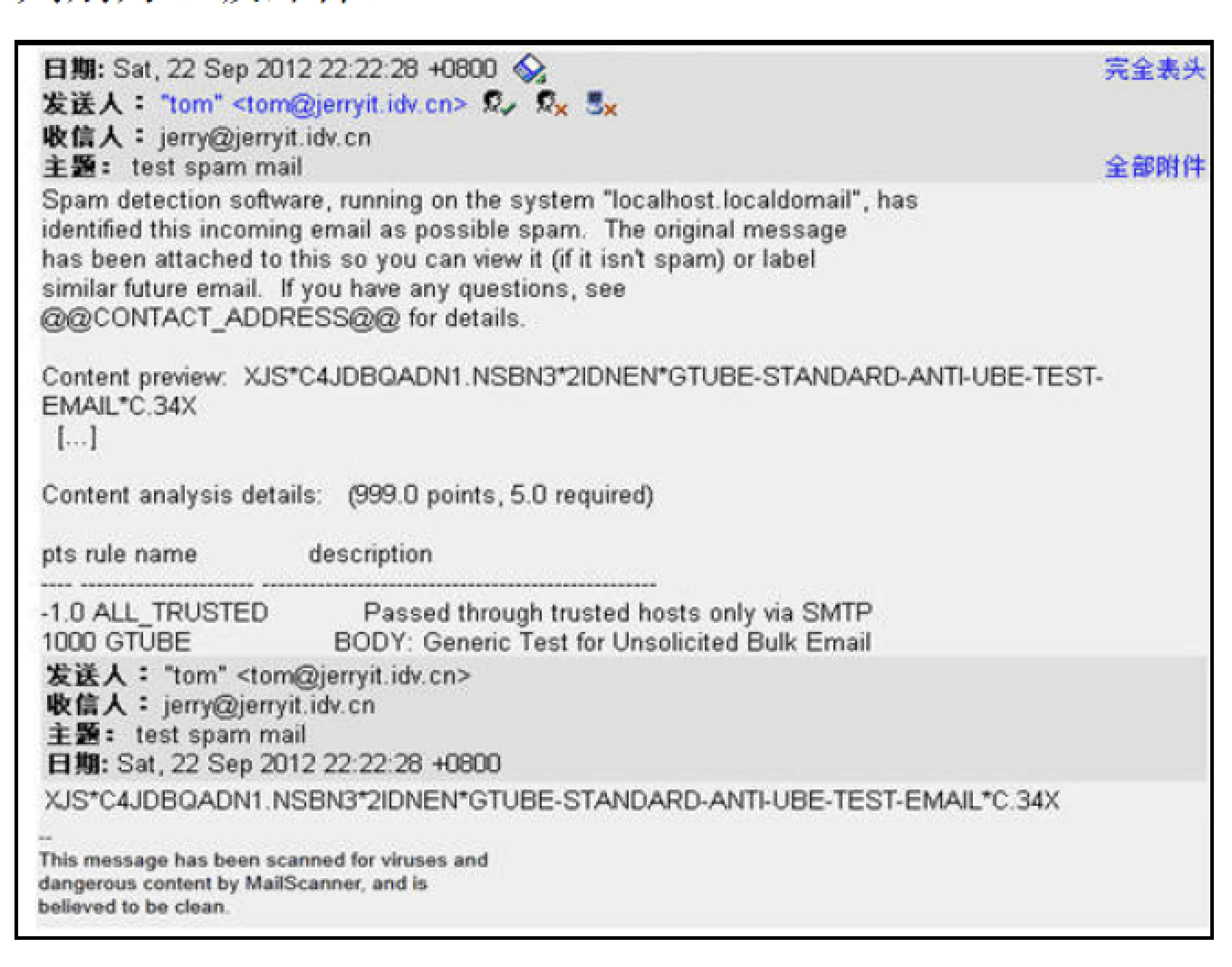
```
[root@localhost ~]# cat /var/log/maillog
```

```
Sep 22 22:27:22 localhost MailScanner[13963]: New Batch: Scanning 1 messages, 1237 bytes
Sep 22 22:27:22 localhost MailScanner[13963]: Virus and Content Scanning: Starting
Sep 22 22:27:23 localhost MailScanner[13963]: Spam Checks: Found 1 spam messages
Sep 22 22:27:23 localhost MailScanner[13963]: Deleted 1 messages from processing-database
```

检查完日志文件后，利用jerry账号登录，OpenWebMail马上弹出信息通知有一封广告邮件，则代表没有被删除。




进入广告邮箱打开邮件，如下图所示，系统会通知垃圾邮件分数高达999.0，比标准值5分高出太多，所以判别为垃圾邮件。




## 22.3 MailScanner+ClamAV防病毒软件

Clamav官方网站：http://www.clamav.net/lang/en/。

MailScanner可以搭配防病毒软件扫描邮件，目前最常用的是ClamAV。

前面介绍了如何将SpamAssassin和MailScanner搭配使用，下面介绍MailScanner如何搭配防病毒软件ClamAV，使邮件服务器更加安全。

### 下载ClamAV防毒软件

ClamAV软件必须自行下载安装，无法使用YUM在线更新方式安装，ClamAV所要安装的软件有4个，分别是clamav、clamav-db、clamav-devel、clamd，可使用wget命令依次下载。

```
[root@localhost ~]# wget
http://pkgs.repoforge.org/clamav/clamav-0.97.2-1.el6.rf.x86_64.rpm
…中间省略…
[root@localhost ~]# wget
http://pkgs.repoforge.org/clamav/clamav-db-0.97.2-1.el6.rf.x86_64.rpm
…中间省略…
[root@localhost ~]# wget
http://pkgs.repoforge.org/clamav/clamav-devel-0.97.2-1.el6.rf.x86_64.rpm
…中间省略…
[root@localhost ~]# wget
http://pkgs.repoforge.org/clamav/clamd-0.97.2-1.el6.rf.x86_64.rpm
…中间省略…
```

说明

文件来源：http://pkgs.repoforge.org/clamav/。

## 安装ClamAV防毒软件

ClamAV软件下载完成后，必须要安装ClamAV的必备软件libtool-ltdl，可以使用YUM在线更新方式安装。

```
[root@localhost ~]# yum -y install libtool-ltdl
Dependencies Resolved
=======================================================================
 Package                Arch         Version           Repository      Size
=======================================================================
Installing:
 libtool-ltdl         x86_64      2.2.6-15.5.el6       base             44 k
Transaction Summary
=======================================================================
Install       1 Package (s)
Upgrade       0 Package (s)
Total download size: 44 k
```

安装好libtool-ltdl软件后，就可以安装ClamAV防毒软件了，ClamAV的4个软件一定要同时安装，否则可能安装失败。

```
 [root@localhost ~]# rpm -ivh clamav-0.97.2-1.el6.rf.x86_64.rpm
clamav-db-0.97.2-1.el6.rf.x86_64.rpm clamav-devel-0.97.2-1.el6.rf.x86_64.rpm
clamd-0.97.2-1.el6.rf.x86_64.rpm
warning: clamav-0.97.2-1.el6.rf.x86_64.rpm: Header V3 DSA/SHA1 Signature, key ID
6b8d79e6: NOKEY
Preparing...            ########################################### [100%]
   1:clamav-db          ########################################### [ 25%]
   2:clamav             ########################################### [ 50%]
   3:clamd              ########################################### [ 75%]
   4:clamav-devel       ########################################### [100%]
```

此错误为未安装libtool-ltdl软件，不过个安装ClamAV基本软件时，也会出现以下类似的信息。

```
[root@localhost ~]# rpm -ivh clamav-0.97.2-1.el6.rf.x86_64.rpm
clamav-db-0.97.2-1.el6.rf.x86_64.rpm clamav-devel-0.97.2-1.el6.rf.x86_64.rpm
clamd-0.97.2-1.el6.rf.x86_64.rpm
warning: clamav-0.97.2-1.el6.rf.x86_64.rpm: Header V3 DSA/SHA1 Signature, key ID
6b8d79e6: NOKEY
error: Failed dependencies:
        libltdl.so.7 () (64bit) is needed by clamav-0.97.2-1.el6.rf.x86_64
```

## 启动ClamAV服务

安装ClamAV软件完成后，就可以启用ClamAV服务了，由于要搭配MailSacnner使用，所以需要将ClamAV服务设为系统默认启动。

```
[root@localhost ~]# service clamd start    //ClamAV 启动
Starting Clam AntiVirus Daemon: Bytecode: Security mode set to "TrustSigned".
LibClamAV Warning: **************************************************
LibClamAV Warning: ***  The virus database is older than 7 days!  ***
LibClamAV Warning: ***   Please update it as soon as possible.    ***
LibClamAV Warning: **************************************************
                                                            [  OK  ]
[root@localhost ~]# chkconfig clamd on                //ClamAV 设为默认启动
```

## 测试ClamAV

ClamAV防毒服务内有模板可以测试扫描，第一次安装好ClamAV服务后，防毒扫描系统会通知病毒数据库太旧，就会有如下所示的扫描结果。

```
[root@localhost ~]# clamscan /usr/share/doc/clamav-*/test/
LibClamAV Warning: **************************************************
LibClamAV Warning: ***  The virus database is older than 7 days!  ***
LibClamAV Warning: ***   Please update it as soon as possible.    ***
LibClamAV Warning: **************************************************
WARNING: /usr/share/doc/clamav-*/test/: Can't access file
/usr/share/doc/clamav-*/test/: No such file or directory
----------- SCAN SUMMARY -----------
Known viruses: 1006584            //病毒特征数量
Engine version: 0.97.2            //ClamAV 版本
Scanned directories: 0            //扫瞄几个目录
Scanned files: 0                  //扫瞄几个文件
Infected files: 0                 //总共有几只感染的文件
Data scanned: 0.00 MB             //数据扫描容量
Data read: 0.00 MB (ratio 0.00:1) //数据读取容量
Time: 3.978 sec (0 m 3 s)         //扫描所花时间
```

如果使用ClamAV防毒服务对整个系统扫描的话，可以输入【clamscan / -r】，不过扫描时

间会很久，建议扫描前更新一下ClamAV病毒特征。

## 更新ClamAV病毒数据库

完成ClamAV服务的安装后，因病毒特征是最旧的，所以建议立即更新，更新的命令如下：

```
[root@localhost ~]# freshclam                              //更新病毒数据库
ClamAV update process started at Wed Sep 21 22:20:53 2011
WARNING: DNS record is older than 3 hours.
WARNING: Invalid DNS reply. Falling back to HTTP mode.
Reading CVD header (main.cvd) : OK (IMS)
main.cvd is up to date (version: 53, sigs: 846214, f-level: 53, builder: sven)
Reading CVD header (daily.cvd) : OK
WARNING: getfile: daily-13357.cdiff not found on remote server (IP: 168.143.19.95)
WARNING: getpatch: Can't download daily-13357.cdiff from db.us.clamav.net
WARNING: getfile: daily-13357.cdiff not found on remote server (IP: 194.186.47.19)
WARNING: getpatch: Can't download daily-13357.cdiff from db.us.clamav.net
WARNING: getfile: daily-13357.cdiff not found on remote server (IP: 64.246.134.219)
WARNING: getpatch: Can't download daily-13357.cdiff from db.us.clamav.net
WARNING: Incremental update failed, trying to download daily.cvd
Downloading daily.cvd [100%]
daily.cvd updated (version: 13653, sigs: 194598, f-level: 60, builder: jesler)
Downloading bytecode.cvd [100%]
bytecode.cvd updated (version: 144, sigs: 41, f-level: 60, builder: edwin)
Database updated (1040853 signatures) from db.us.clamav.net (IP: 69.163.100.14)
Clamd successfully notified about the update.
```

## 配置每天自动更新病毒特征

修改freshclam配置文件内的Checks参数，该参数默认未启用，将【#】号删除，则Clam Antivirus每24小时更新一次，即每天更新一次。

```
[root@localhost ~]# vi /etc/freshclam.conf
# Number of database checks per day.
# Default: 12 (every two hours)
Checks 24                        //默认未启用，将#号删除，默认为 24 小时更新一次
```

## 配置MailScanner搭配ClamAV防毒进行扫描

配置MailScanner服务搭配防病毒软件进行扫描，对MailScanner配置文件中的Virus Scanning参数进行修改，默认为yes，表示使用防病毒软件扫描，设为no则不使用。

```
[root@localhost ~]# vi /etc/MailScanner/MailScanner.conf
# Do you want to scan email for viruses?
# A few people don't have a virus scanner licence and so want to disable
# all the virus scanning.
# If you use a ruleset for this setting, then the mail will be scanned if
```

```
# *any* of the rules match (except the default) . That way unscanned mail
# never reaches a user who is having their mail virus-scanned.
#
# If you want to be able to switch scanning on/off for different users or
# different domains, set this to the filename of a ruleset.
# This can also be the filename of a ruleset.
Virus Scanning = yes                                          //默认为 yes
```

修改Virus Scanning参数配置为yes，表示使用防病毒软件，接下来要配置MailScanner所搭配使用的防病毒软件的名称，Virus Scanners参数为配置防病毒软件名称，默认为auto，自动选择，现在要搭配ClamAV服务使用，则将防病毒软件名称修改成ClamAV。

```
[root@localhost ~]# vi /etc/MailScanner/MailScanner.conf
# Note: If you want to use multiple virus scanners, then this should be a
#       space-separated list of virus scanners. For example:
#       Virus Scanners = sophos f-prot mcafee
#
# Note: Make sure that you check that the base installation directory in the
#       3rd column of virus.scanners.conf matches the location you have
#       installed each of your virus scanners. The supplied
#       virus.scanners.conf file assumes the default installation locations
#       recommended by each of the virus scanner installation guides.
#
# Note: If you specify "auto" then MailScanner will search for all the
#       scanners you have installed and will use all of them. If you really
#       want none, then specify "none".
#
# This *cannot* be the filename of a ruleset.
Virus Scanners = clamav             //默认为 auto，配置为所要使用的防病毒软件名称
```

配置完成后，必须重新启动MailScanner服务，才可以与ClamAV搭配使用。

```
[root@localhost ~]# service MailScanner restart
Shutting down MailScanner daemons:
         MailScanner:                                       [  OK  ]
         incoming postfix:                                  [  OK  ]
         outgoing postfix:                                  [  OK  ]
Waiting for MailScanner to die gracefully ... dead.
Starting MailScanner daemons:
         incoming postfix:                                  [  OK  ]
         outgoing postfix:                                  [  OK  ]
         MailScanner:                                       [  OK  ]
```

## MailScanner搭配ClamAV使用测试

配置好MailScanner使用ClamAV防毒后，可发送一封病毒邮件测试配置是否生效，病毒邮件内容如下。

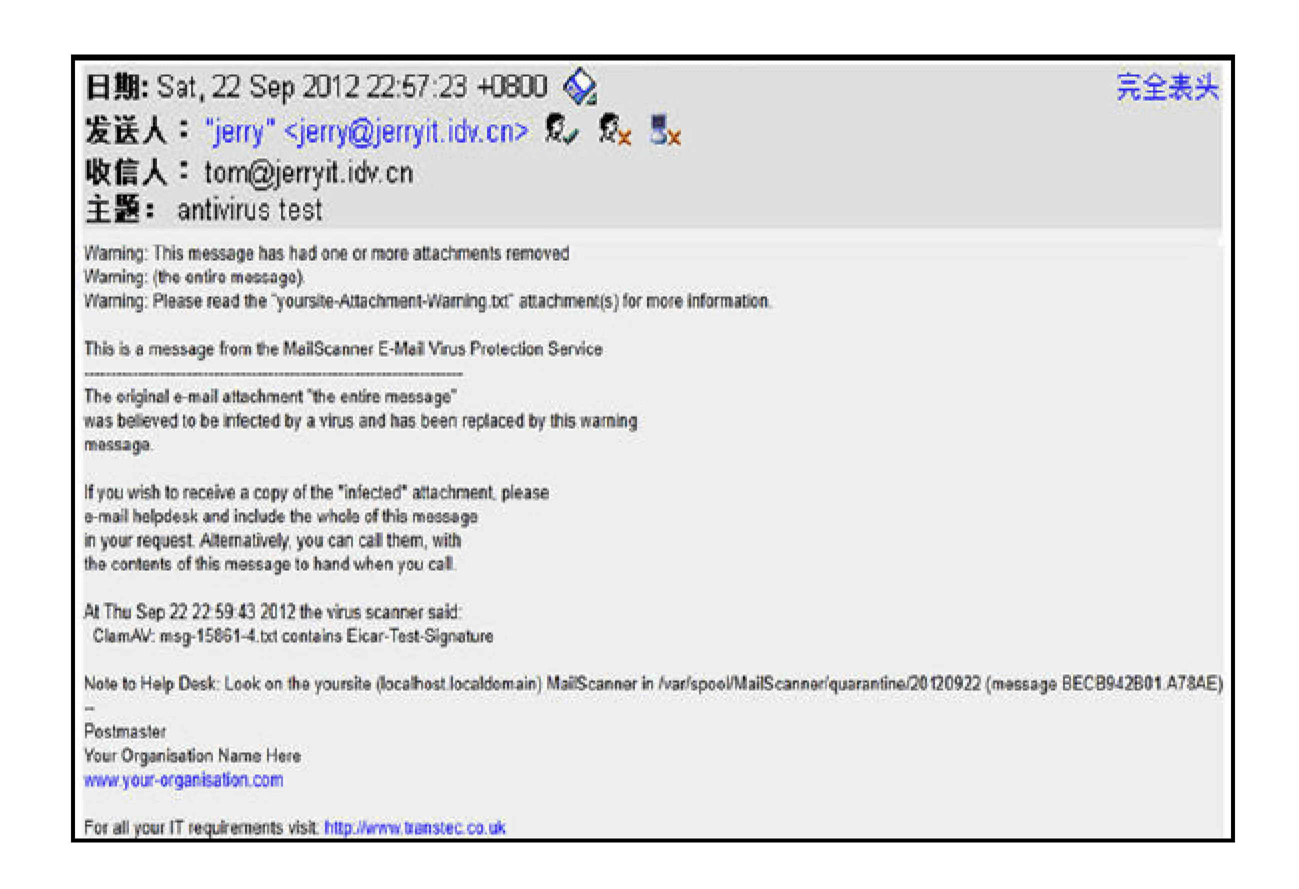
| 病毒邮件内容 |
|---|
| X5O!P%@AP[4\PZX54（P^）7CC）7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* |




邮件发送后，检查邮件日志文件，若出现Virus and Content Scanning: Starting代表防病毒软件已启动扫描。

```
[root@localhost ~]# cat /var/log/maillog
Sep 22 22:57:23 localhost postfix/pipe[15907]: F3F3842B14: to=<tom@jerryit.idv.cn>,
relay=spamassassin, delay=5.9, delays=4.8/0/0/1.1, dsn=2.0.0, status=sent (delivered via
spamassassin service)
Sep 22 22:57:23 localhost postfix/qmgr[15850]: F3F3842B14: removed
Sep 22 22:57:23 localhost MailScanner[15872]: New Batch: Found 2 messages waiting
Sep 22 22:57:23 localhost MailScanner[15872]: New Batch: Scanning 1 messages, 2452 bytes
Sep 22 22:57:23 localhost MailScanner[15872]: Virus and Content Scanning: Starting
Sep 22 22:57:24 localhost MailScanner[15861]: Requeue: 8C24F42B15.A4BF6 to C34E442B1F
Sep 22 22:57:24 localhost postfix/qmgr[15850]: C34E442B1F:
from=<postmaster@mail.jerryit.idv.cn>, size=1366, nrcpt=1 (queue active)
Sep 22 22:57:24 localhost MailScanner[15861]: Uninfected: Delivered 1 messages
Sep 22 22:57:25 localhost postfix/local[15920]: C34E442B1F:
to=<root@mail.jerryit.idv.cn>, orig_to=<postmaster>, relay=local, delay=4.5,
delays=4.4/0/0/0.04, dsn=2.0.0, status=sent (delivered to mailbox)
Sep 22 22:57:25 localhost postfix/qmgr[15850]: C34E442B1F: removed
Sep 22 22:57:25 localhost MailScanner[15861]: Deleted 1 messages from processing-database
Sep 22 22:57:24 localhost MailScanner[15872]: Requeue: 9DA4542B1A.A9587 to DF74A42B01
Sep 22 22:57:24 localhost postfix/qmgr[15850]: DF74A42B01:
from=<jerry@localhost.localdomain>, size=2222, nrcpt=1 (queue active)
Sep 22 22:57:24 localhost MailScanner[15872]: Uninfected: Delivered 1 messages
Sep 22 22:57:24 localhost postfix/local[15920]: DF74A42B01: to=<tom@jerryit.idv.cn>,
relay=local, delay=5, delays=4.9/0/0/0.09, dsn=2.0.0, status=sent (delivered to mailbox)
Sep 22 22:57:24 localhost postfix/qmgr[15850]: DF74A42B01: removed
Sep 22 22:57:24 localhost MailScanner[15872]: Deleted 1 messages from processing-database
Sep 22 23:01:03 localhost update.bad.phishing.sites: Delaying cron job up to 600 seconds
```

当收件人接收邮件时会收到一封主题为antivirus test的邮件，提示邮件内容有病毒，这就表示MailScanner搭配ClamAV配置成功。




## 22.4 使用MailScanner阻挡钓鱼邮件

钓鱼邮件是指利用伪装的电邮，欺骗收件人将账号、密码等信息回复给指定的按收者，或引导收件人链接到特制的网页，这些网页通常会伪装成和真实网站一样，实际上它的链接与邮件内的网址不相符，误导用户使用假冒的网站，进而对收件人进行行骗。可以利用MailScanner过滤邮件内容，如果有这样的邮件，会将该邮件阻挡。

### 检查MailScanner配置

检查MailScanner配置中对钓鱼邮件的检查是否开启，Find Phishing Fraud参数默认为yes启动，如果看到no的设置，将其改成yes。

```
[root@localhost ~]# vi /etc/MailScanner/MailScanner.conf
# Do you want to check for "Phishing" attacks?
# These are attacks that look like a genuine email message from your bank,
# which contain a link to click on to take you to the web site where you
# will be asked to type in personal information such as your account number
# or credit card details.
# Except it is not the real bank's web site at all, it is a very good copy
# of it run by thieves who want to steal your personal information or
# credit card details.
# These can be spotted because the real address of the link in the message
# is not the same as the text that appears to be the link.
# Note: This does cause extra load, particularly on systems receiving lots
#       of spam such as secondary MX hosts.
# This can also be the filename of a ruleset.
Find Phishing Fraud = yes    //是否检测钓鱼邮件，yes 为启动，no 为不启动
…中间省略…
# While detecting "Phishing" attacks, do you also want to point out links
# to numeric IP addresses. Genuine links to totally numeric IP addresses
# are very rare, so this option is set to "yes" by default. If a numeric
# IP address is found in a link, the same phishing warning message is used
# as in the Find Phishing Fraud option above.
```

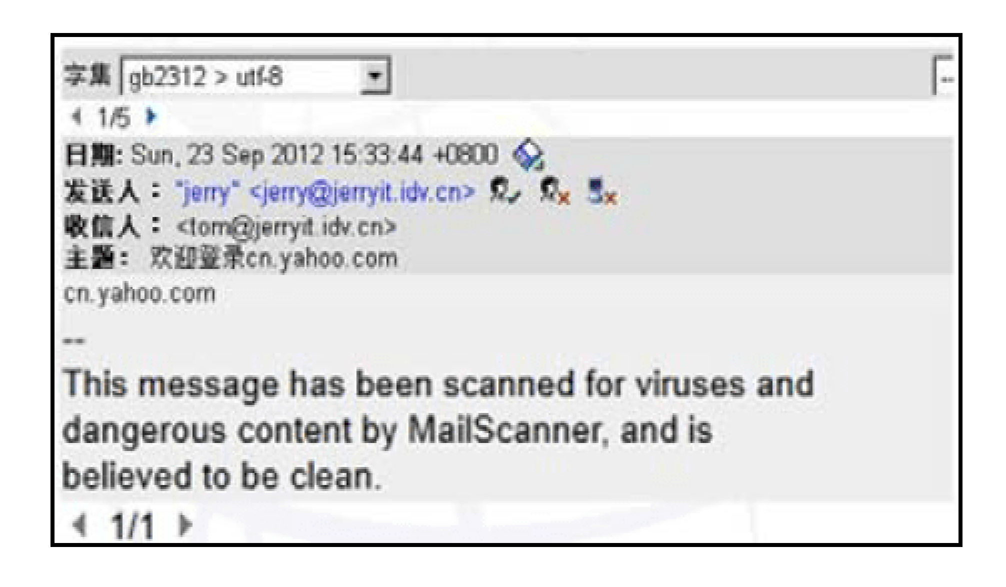
```
# This can also be the filename of a ruleset.
Also Find Numeric Phishing = yes   //是否检测 IP 方式的连结
…中间省略…
# If a phishing fraud is detected, do you want to highlight the tag with
# a message stating that the link may be to a fraudulent web site.
# This can also be the filename of a ruleeset.
Highlight Phishing Fraud = yes //配置检测到钓鱼邮件时，在邮件中加上警告信息
```

完成修改配置后，建议重新启动MailScanner服务。

```
[root@localhost ~]# service MailScanner restart
Shutting down MailScanner daemons:
         MailScanner:                                      [  OK  ]
         incoming postfix:                                 [  OK  ]
         outgoing postfix:                                 [  OK  ]
Waiting for MailScanner to die gracefully ... dead.
Starting MailScanner daemons:
         incoming postfix:                                 [  OK  ]
         outgoing postfix:                                 [  OK  ]
         MailScanner:                                      [  OK  ]
```

## 测试钓鱼邮件

利用jerry用户写一封邮件给tom用户，内容输入【欢迎登录cn.yahoo.com】，故意将cn.yahoo.com超链接配置为ccn.yahoo.com，如果MailScanner服务检测为钓鱼邮件，系统就会将它阻挡，如下图所示。



# 第四部分

# 网络流量监控工具篇

# 第23章

# Bandwidthd——网络流量分析统计

Bandwidthd官方网站：http://bandwidthd.sourceforge.net/。

Bandwidthd是一套免费的网络流量监控统计软件，监控网络流量行为并以图形及统计表的方式显示，可以区分FTP、HTTP、P2P、TCP、UDP、ICMP等行为，并以天、星期、月、年来统计，bandwidthd算是MIS管理和监控网络的好帮手。

下载地址：http://sourceforge.net/projects/bandwidthd/files/。

目前最新版本为bandwidthd-2.0.1。

## 23.1 安装必备软件

Bandwidthd工具显示统计流量，需要使用Apache服务，除此之外还有其他组件，如gcc、libpng、libpng-devel、gd、gd-devel、libpcap-devel，建议使用YUM在线更新方法安装。

```
[root@localhost ~]# yum install -y httpd gcc libpng libpng-devel gd gd-devel
 libpcap-devel
Dependencies Resolved
==========================================================================
 Package           Arch       Version                Repository       Size
==========================================================================
Installing:
 gcc                 x86_64   4.4.4-13.el6             base         10 M
 gd                  x86_64   2.0.35-10.el6            base        142 k
 gd-devel            x86_64   2.0.35-10.el6            base         78 k
 httpd               x86_64   2.2.15-5.el6.centos      base        811 k
 libpcap-devel       x86_64   14:1.0.0-6.20091201git117cb5.el6   base   97 k
 libpng-devel        x86_64   2:1.2.44-1.el6           base        111 k
Installing for dependencies:
 apr                 x86_64   1.3.9-3.el6_0.1          updates     124 k
 apr-util            x86_64   1.3.9-3.el6_0.1          updates      87 k
 apr-util-ldap       x86_64   1.3.9-3.el6_0.1          updates      15 k
 cloog-ppl           x86_64   0.15.7-1.2.el6           base         93 k
```

```
 cpp                  x86_64    4.4.4-13.el6               base        3.7 M
 fontconfig-devel     x86_64    2.8.0-3.el6                base        209 k
 freetype-devel      x86_64    2.3.11-6.el6_0.2           updates     363 k
 glibc-devel          x86_64    2.12-1.7.el6_0.5           updates     961 k
 glibc-headers        x86_64    2.12-1.7.el6_0.5           updates     592 k
 httpd-tools          x86_64    2.2.15-5.el6.centos        base         68 k
 kernel-headers       x86_64    2.6.32-71.29.1.el6         updates     991 k
 libX11-devel         x86_64    1.3-2.el6                  base        1.0 M
 libXau-devel         x86_64    1.0.5-1.el6                base         13 k
 libXdmcp             x86_64    1.0.3-1.el6                base         22 k
 libXdmcp-devel       x86_64    1.0.3-1.el6                base        9.6 k
 libXpm               x86_64    3.5.8-2.el6                base         59 k
 libXpm-devel         x86_64    3.5.8-2.el6                base         33 k
 libXt                x86_64    1.0.7-1.el6                base        174 k
 libjpeg-devel        x86_64    6b-46.el6                  base        100 k
 libxcb-devel         x86_64    1.5-1.el6                  base        139 k
 mpfr                 x86_64    2.4.1-6.el6                base        157 k
 ppl                  x86_64    0.10.2-11.el6              base        1.3 M
 xorg-x11-proto-devel noarch 7.4-35.el6                    base        250 k
 zlib-devel           x86_64    1.2.3-25.el6               base         43 k
Updating for dependencies:
 freetype             x86_64    2.3.11-6.el6_0.2           updates     359 k
 glibc                x86_64    2.12-1.7.el6_0.5           updates     3.7 M
 glibc-common         x86_64    2.12-1.7.el6_0.5           updates      14 M
Transaction Summary
=========================================================================
Install       30 Package(s)
Upgrade        3 Package(s)
Total download size: 40 M
```

## 23.2 安装Bandwidthd 软件

使用wget命令下载Bandwidthd软件，下载完成后，解压缩并安装Bandwidthd，由于安装文件为tar压缩文件，所以必须进行编译安装。

```
[root@localhost ~]# wget http://downloads.sourceforge.net/project/
bandwidthd/bandwidthd/bandwidthd%202.0.1/bandwidthd-2.0.1.tgz   //下载 bandwidthd
[root@localhost ~]# tar -zxvf bandwidthd-2.0.1.tgz              //解压缩文件
…中间省略…
[root@localhost ~]# cd bandwidthd*                              //进入 bandwidthd 安装目录
[root@localhost bandwidthd-2.0.1]# ./configure
…中间省略…
[root@localhost bandwidthd-2.0.1]# make
…中间省略…
[root@localhost bandwidthd-2.0.1]# make install                 //编译并安装软件
…中间省略…
```

> 说明
>
> 注意【./configure】前面有一个小数点。

下表为bandwidthd的相关路径说明。

| 目录名称 | 路径 |
|---|---|
| 默认程序安装目录 | /usr/local/bandwidthd |
| bandwidthd 配置文件 | /usr/local/bandwidthd/etc/bandwidthd.conf |
| bandwidthd 网页目录 | /usr/local/bandwidthd/htdocs |

## 配置Bandwidthd监控网段

要使用Bandwidthd工具，必须先配置要监控的网段，才会对监控网段进行检测，编辑bandwidthd配置文件，例如，要检测192.168.233网段，Bandwidthd只会监控检测192.168.233.1~192.168.233.254的所有IP地址流量，配置负责监控流量的网卡，默认为eth0，若有两块网卡，想要使用第二块网卡eth1进行检测，可以将其修改成eth1。

```
[root@localhost ~]# vi /usr/local/bandwidthd/etc/bandwidthd.conf
####################################################
# Bandwidthd.conf
#
# Commented out options are here to provide
# documentation and represent defaults
# Subnets to collect statistics on.  Traffic that
# matches none of these subnets will be ignored.
# Syntax is either IP Subnet Mask or CIDR
#subnet 10.0.0.0 255.0.0.0      //默认这三段加上#号停止检测
#subnet 192.168.233.0/16
#subnet 172.16.0.0/12
subnet 192.168.233.0/24        //检测 192.168.233 网段，其他网段依此类推
# Device to listen on
# Bandwidthd listens on the first device it detects
# by default.  Run "bandwidthd -l" for a list of
# devices.
dev "eth0"                     //将#号移除后，以 eth0 网卡检测，或者可配置其他网卡
```

> 说明
>
> 配置的网络地址须与要监控的网络是同一网段，否则无法监控流量。

## 建立Bandwidthd网页链接

进入Apache网页目录，使用ln命令链接bandwidthd目录，这样就不用输入一长串的路径了。

```
[root@localhost ~]# cd /var/www/html                          //进入 Apache 默认目录
[root@localhost html]# ln -s /usr/local/bandwidthd/htdocs bandwidthd
                                                              //配置 bandwidthd 网页链接
[root@localhost html]# ll                                     //检查是否建立链接
total 0
lrwxrwxrwx. 1 root root 28 Sep  3 20:48 bandwidthd -> /usr/local/bandwidthd/htdocs
```

## 配置Bandwidthd为默认启动

每次机器重新启动时，必须自动启动Bandwidthd，所以必须将Bandwidthd设为开机默认启动。由于Bandwidthd不是系统服务，所以需要添加到rc.local文件，才可以默认启动。

```
[root@localhost html]# vi /etc/rc.local    //编辑 rc.local 配置默认启动
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
/usr/local/bandwidthd/bandwidthd           //配置 bandwidthd 为默认启动
```

## 启动Bandwidthd服务

进入bandwidthd目录，启动bandwidthd服务，启动命令是【./ bandwidthd】，若要停止bandwidthd服务，输入【killall bandwidthd】。

```
[root@localhost html]# cd /usr/local/bandwidthd   //进入 bandwidthd 目录
[root@localhost bandwidthd]# ./bandwidthd         //启动 bandwidthd
```

> **说明**
> 加入新的检测监控网段需要先停止bandwidthd，加入完后再启动。

下表为bandwidthd的启动停止方式。

| 操作说明 | 操作命令 |
|---|---|
| bandwidthd 启动 | ./bandwidthd |
| bandwidthd 停止 | killall  bandwidthd |

## 配置防火墙

Bandwidthd需使用Apache服务，所以必须在防火墙配置中开启80端口。

```
[root@localhost bandwidthd]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
```

```
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost bandwidthd]# service iptables restart
iptables: Flushing firewall rules:                  [  OK  ]
iptables: Setting chains to policy ACCEPT: filter   [  OK  ]
iptables: Unloading modules:                        [  OK  ]
iptables: Applying firewall rules:                  [  OK  ]
```

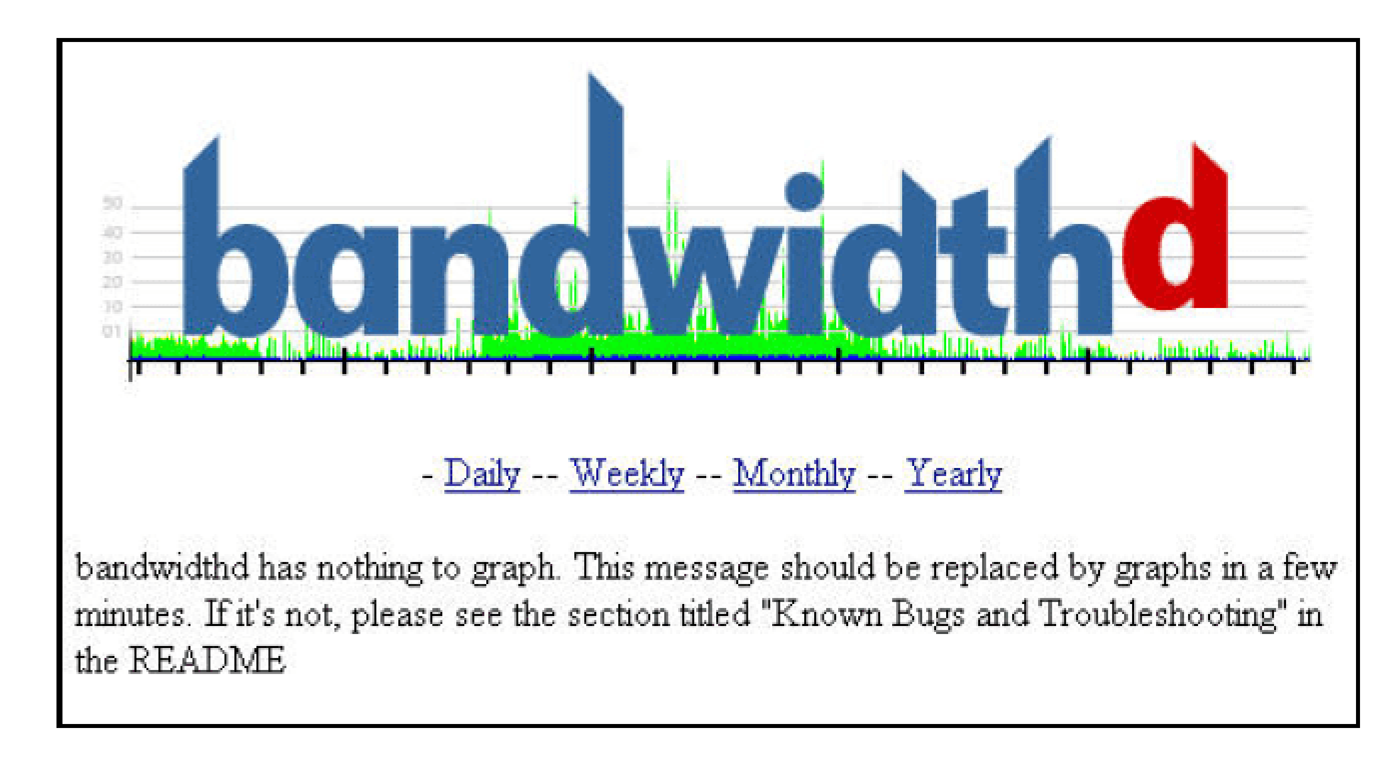
### 启动Apache服务

将Apache配置为默认启动，因为Bandwidthd要不断检测监控网段，所以重新启动系统后也要自动启动。

```
[root@localhost ]# service httpd start      //启动 Apache
Starting httpd:                 [  OK  ]
[root@localhost ~]# chkconfig httpd on      //将 Apache 设为默认启动
```

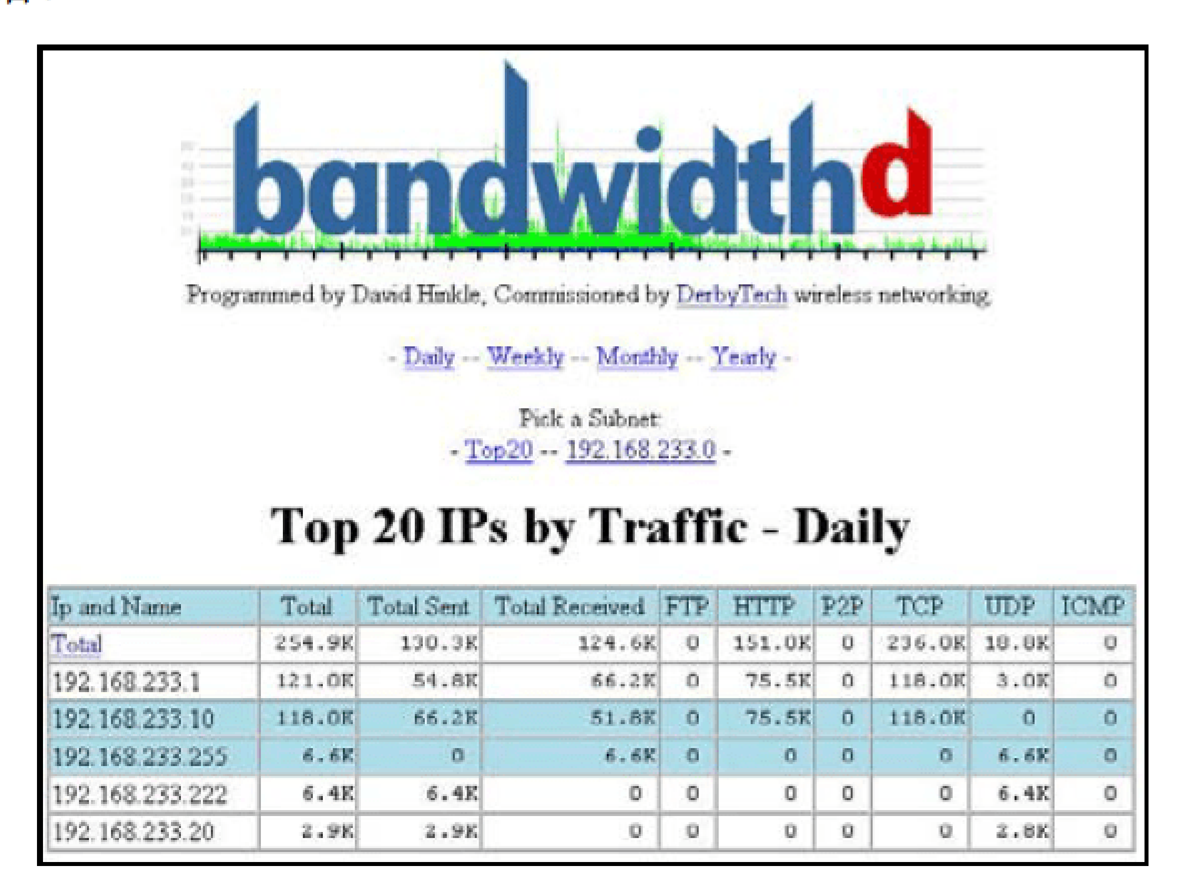
## 23.3 开始使用Bandwidthd

在浏览器中输入【http://IP地址/bandwidthd】，第一次使用会出现以下信息，代表目前正在收集信息，重新加入新的网段后，打开浏览器也会出现此信息。



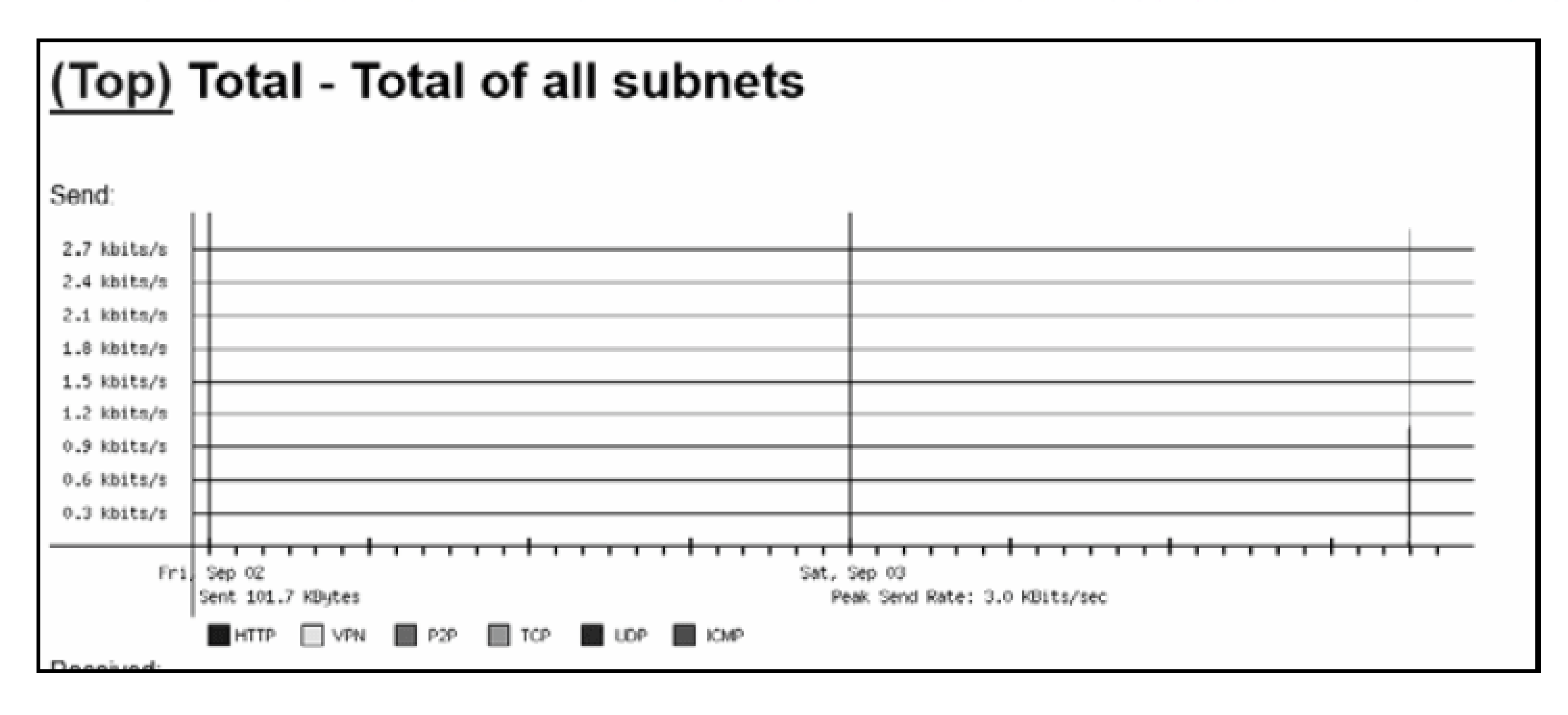

花几分钟收集数据，Bandwidthd就会检测出所配置的网段IP地址流量，也可以以天、星期、

月、年为单位统计数据。




| Ip and Name | Total | Total Sent | Total Received | FTP | HTTP | P2P | TCP | UDP | ICMP |
|---|---|---|---|---|---|---|---|---|---|
| Total | 254.9K | 130.3K | 124.6K | 0 | 151.0K | 0 | 236.0K | 18.8K | 0 |
| 192.168.233.1 | 121.0K | 54.8K | 66.2K | 0 | 75.5K | 0 | 118.0K | 3.0K | 0 |
| 192.168.233.10 | 118.0K | 66.2K | 51.8K | 0 | 75.5K | 0 | 118.0K | 0 | 0 |
| 192.168.233.255 | 6.6K | 0 | 6.6K | 0 | 0 | 0 | 0 | 6.6K | 0 |
| 192.168.233.222 | 6.4K | 6.4K | 0 | 0 | 0 | 0 | 0 | 6.4K | 0 |
| 192.168.233.20 | 2.9K | 2.9K | 0 | 0 | 0 | 0 | 0 | 2.8K | 0 |

Bandwidthd不光使用图形界面显示监控数据，也使用统计数据方式显示监控数据。



# 第24章

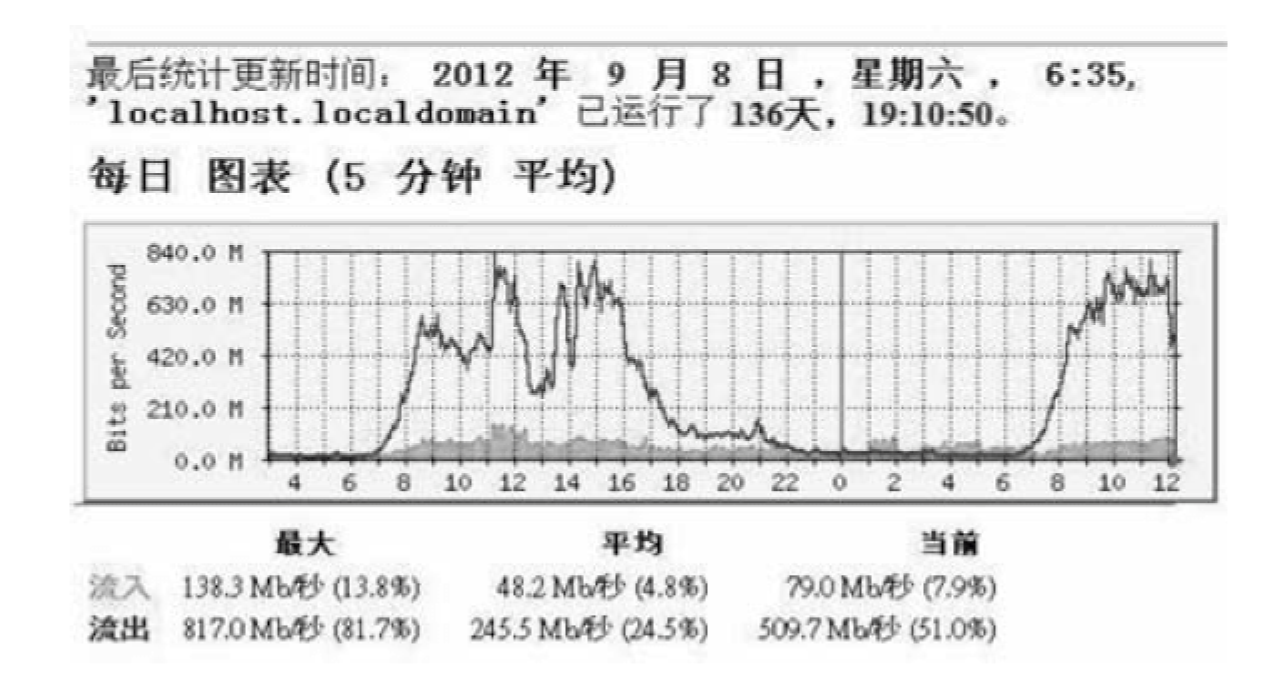
# MRTG——网络流量分析统计

MRTG 官方网站：http://oss.oetiker.ch/mrtg/。

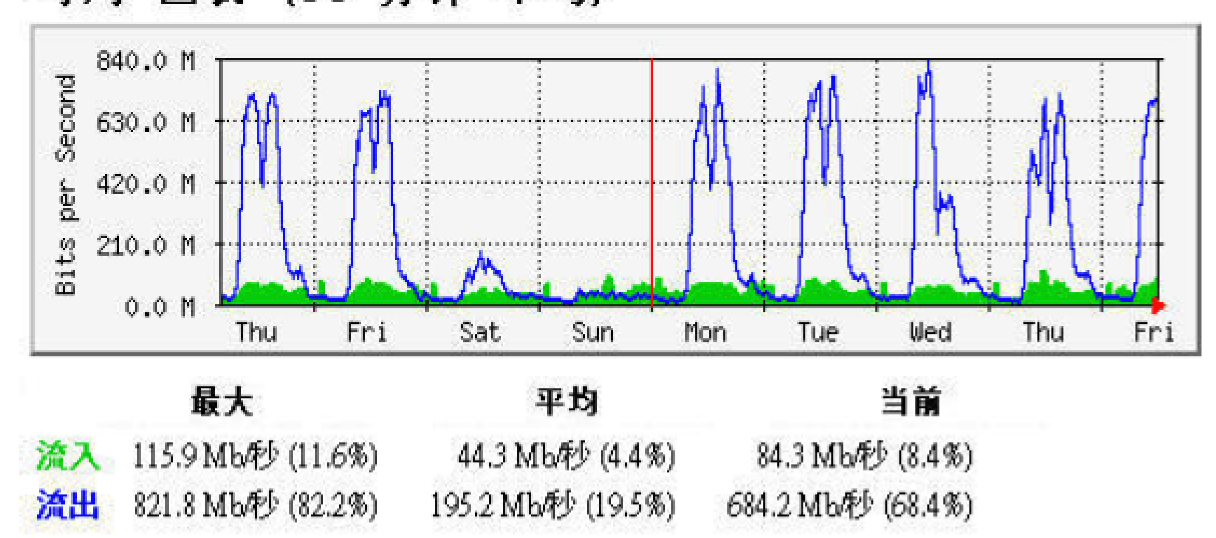
MRTG（Multi Router Traffic Grapher）是一款可用来绘制网络流量图的软件，由瑞士奥尔滕克的Tobias Oetiker与Dave Rand开发，此软件以GPL授权。

监控设备必须支持SNMP协议。 MRTG以所收集到的数据生成HTML文件，以GIF或PNG格式绘制出图形，并以日、周、月、年等统计时间分别展现。它也可以生成最大值、最小值及平均值供统计使用。

**日流量图**

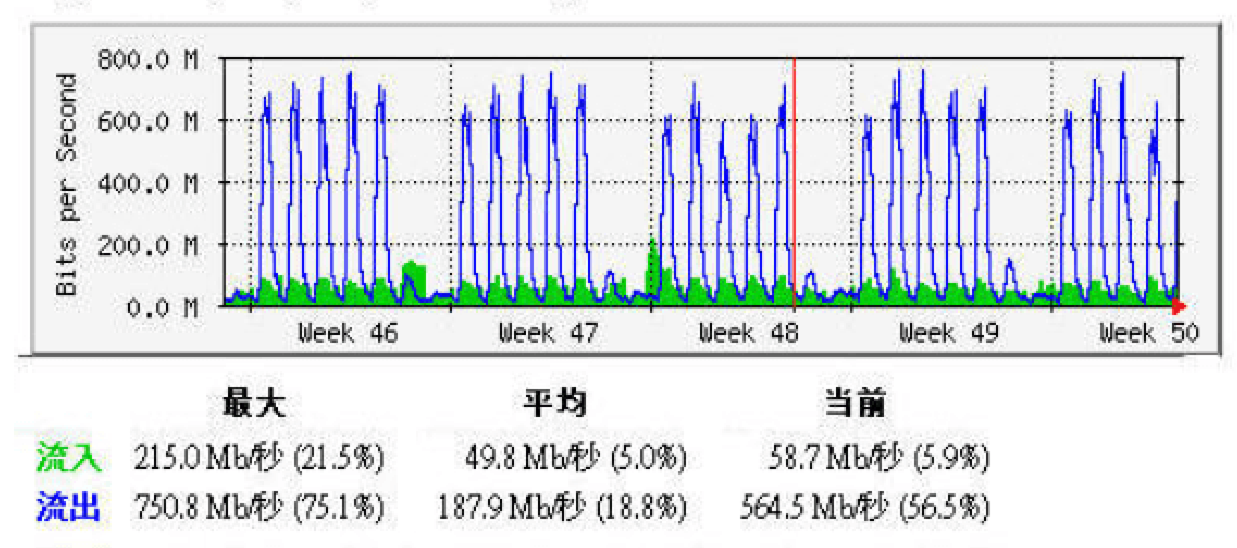



**周流量图**



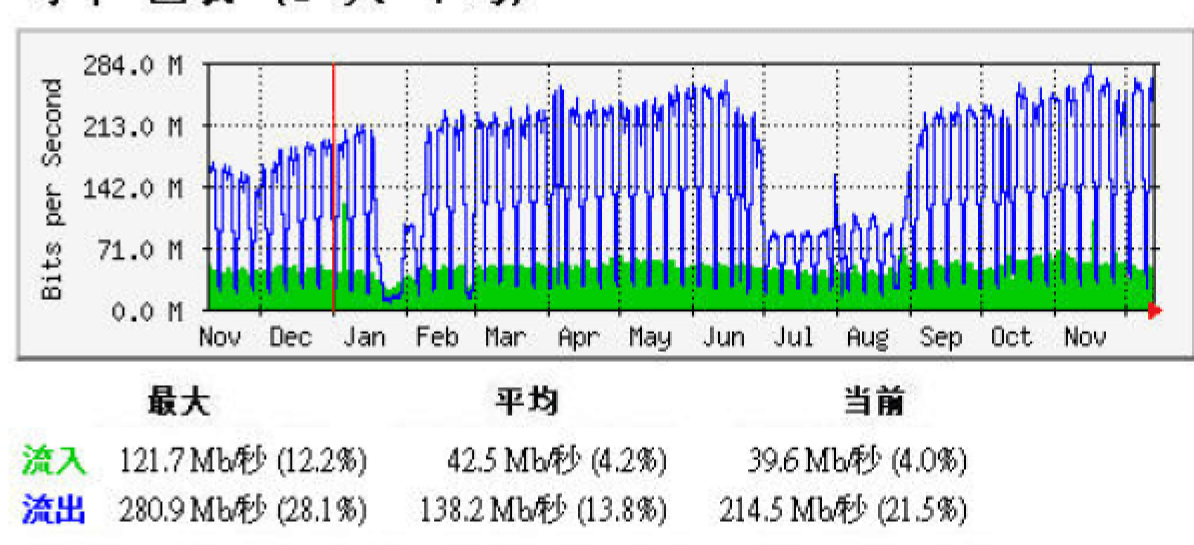
月流量图




年流量图

每年 图表（1 天 平均）




# 24.1 MRTG分析统计本机流量

若要检测本地服务器的网络流量，并生成流量统计图，最重要的是SNMP必须要启动，否则配置完成后，不会出现任何的流量统计图。示例中IP地址为192.168.233.10。

## 安装必备软件

使用MRTG软件必须安装Apache及SNMP服务，可用YUM在线更新方式安装。

```
[root@localhost ~]# yum install -y httpd net-snmp
Dependencies Resolved
======================================================================
 Package          Arch       Version                 Repository      Size
======================================================================
Installing:
 httpd            x86_64     2.2.15-5.el6.centos      base          811 k
 net-snmp         x86_64     1:5.5-27.el6_0.1         updates       297 k
Installing for dependencies:
 apr              x86_64     1.3.9-3.el6_0.1          updates       124 k
 apr-util         x86_64     1.3.9-3.el6_0.1          updates        87 k
 apr-util-ldap    x86_64     1.3.9-3.el6_0.1          updates        15 k
 httpd-tools      x86_64     2.2.15-5.el6.centos      base           68 k
```

```
 lm_sensors-libs x86_64     3.1.1-10.el6            base          37 k
 net-snmp-libs   x86_64     1:5.5-27.el6_0.1        updates       1.5 M
Transaction Summary
==========================================================================
Install       8 Package (s)
Upgrade       0 Package (s)
Total download size: 2.9 M
```

## 配置Apache编码

为了使MRTG软件支持简体中文，需要让Apache服务使用UTF-8编码，所以必须要修改Apache配置文件。

```
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf
#
# Specify a default charset for all content served; this enables
# interpretation of all content as UTF-8 by default.  To use the
# default browser choice (ISO-8859-1) , or to allow the META tags
# in HTML content to override this choice, comment out this
# directive:
#
AddDefaultCharset UTF-8
```

## 编辑SNMP配置文件

安装完SNMP服务后，必须要配置才可以使用，在最后添加View参数。

```
[root@localhost ~]# vi /etc/snmp/snmpd.conf
# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#       name           incl/excl     subtree         mask (optional)
view    systemview    included   .1.3.6.1.2.1.1
view    systemview    included   .1.3.6.1.2.1.25.1.1
view    systemview    included   .1.3.6.1.2.1.2
```

## 启动SNMP 服务

SNMP服务配置完成后，接下来就是启动SNMP服务，并将SNMP服务设为默认启动。

```
[root@localhost ~]# service snmpd start       //启动 SNMP
Starting snmpd:                         [  OK  ]
[root@localhost ~]# chkconfig snmpd on        //SNMP 配置为默认启动
```

## 安装MRTG软件

以前的CentOS版本无法以YUM在线更新的方法安装，不过CentOS 6.0可以由yum方式在线更新方法进行安装。

```
[root@localhost ~]# yum install -y mrtg                    //安装 MRTG 软件
Dependencies Resolved
========================================================================
 Package                Arch       Version             Repository      Size
========================================================================
Installing:
 mrtg                 x86_64    2.16.2-5.el6        base            694 k
Installing for dependencies:
 gd                   x86_64    2.0.35-10.el6       base            142 k
 libXpm               x86_64    3.5.8-2.el6         base             59 k
 mrtg-libs            x86_64    2.16.2-5.el6        base             95 k
 perl-IO-Socket-INET6 noarch  2.56-4.el6          base             17 k
 perl-SNMP_Session    noarch   1.12-4.el6          base             67 k
 perl-Socket6         x86_64    0.23-3.el6          base             23 k
Transaction Summary
========================================================================
Install       7 Package(s)
Upgrade       0 Package(s)
Total download size: 1.1 M
```

## 配置检测来源

配置MRTG检测来源，将Deny from all参数加上#号，如果不添加则无法检测来源，然后添加Allow from all允许检测所有来源。

```
[root@localhost ~]# vi /etc/httpd/conf.d/mrtg.conf
#
# This configuration file maps the mrtg output (generated daily)
# into the URL space.  By default these results are only accessible
# from the local host.
#
Alias /mrtg /var/www/mrtg
<Location /mrtg>
    Order deny,allow
#   Deny from all
    Allow from all              //配置检测所有来源
    Allow from 127.0.0.1
    Allow from ::1
    # Allow from .example.com
</Location>
```

## 生成MRTG配置文件

MRTG配置完成后，就可以使用系统生成MRTG配置文件了，生成MRTG配置文件后，再编辑配置文件。

```
[root@localhost ~]# cfgmaker public@192.168.233.10 > /etc/mrtg/mrtg.cfg
                                              //生成 MRTG 配置文件
[root@localhost ~]# vi /etc/mrtg/mrtg.cfg     //编辑 MRTG 配置文件
# Created by
# /usr/bin/cfgmaker public@192.168.233.10     //被检测主机 IP 地址
### Global Config Options
```

```
#  for UNIX
WorkDir: /var/www/mrtg    //把#号删除，并将路径修改为网站网页目录路径
Refresh:300
Interval:5
Language:zh_CN.UTF-8
options[_]: growright
```

说明

- 示例IP地址为192.168.233.10，请依实际情况修改。
- 若WorkDir: /home/http/mrtg前的#号未删除，则网页生成会失败，找不到目录。

```
[root@localhost mrtg]# env LANG=C mrtg /etc/mrtg/mrtg.cfg
Use of uninitialized value $dir in concatenation (.) or string at /usr/bin/mrtg
line 2530.
Use of uninitialized value $dir in concatenation (.) or string at /usr/bin/mrtg
line 2548.
Use of uninitialized value $dir in concatenation (.) or string at /usr/bin/mrtg
line 2564.
ERROR: "WorkDir" not specified in mrtg config file
```

## 生成MRTG网页

生成MRTG网页时，需要输入三次命令，执行到完全没有错误信息时，才算完成，若三次过后还有错误，就要检查配置文件是否有配置错误。

```
[root@localhost ~]# env LANG=C mrtg /etc/mrtg/mrtg.cfg            //第一次
2012-09-08 15:51:49, Rateup WARNING: /usr/bin/rateup could not read the primary log file
for 192.168.233.10_2
2012-09-08 15:51:49, Rateup WARNING: /usr/bin/rateup The backup log file for
192.168.233.10_2 was invalid as well
2012-09-08 15:51:49, Rateup WARNING: /usr/bin/rateup Can't remove 192.168.233.10_2.old
updating log file
2012-09-08 15:51:49, Rateup WARNING: /usr/bin/rateup Can't rename 192.168.233.10_2.log to
192.168.233.10_2.old updating log file
[root@localhost ~]# env LANG=C mrtg /etc/mrtg/mrtg.cfg            //第二次
2012-09-08 15:51:52, Rateup WARNING: /usr/bin/rateup Can't remove 192.168.233.10_2.old
updating log file
[root@localhost ~]# env LANG=C mrtg /etc/mrtg/mrtg.cfg            //第三次
[root@localhost ~]#
```

## 启动Apache服务

MRTG所有配置完成后，接下来就是启动Apache网页服务器，将Apache设为默认启动。

```
[root@localhost ~]# service httpd start     //启动httpd
Starting httpd:                        [  OK  ]
```

```
[root@localhost ~]# chkconfig httpd on      //Apache 设为默认启动
```

## 配置防火墙

MRTG要用到Apache服务，必须在防火墙配置文件中开启80端口，这样才可以对外连接。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
                                                           //Apache 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

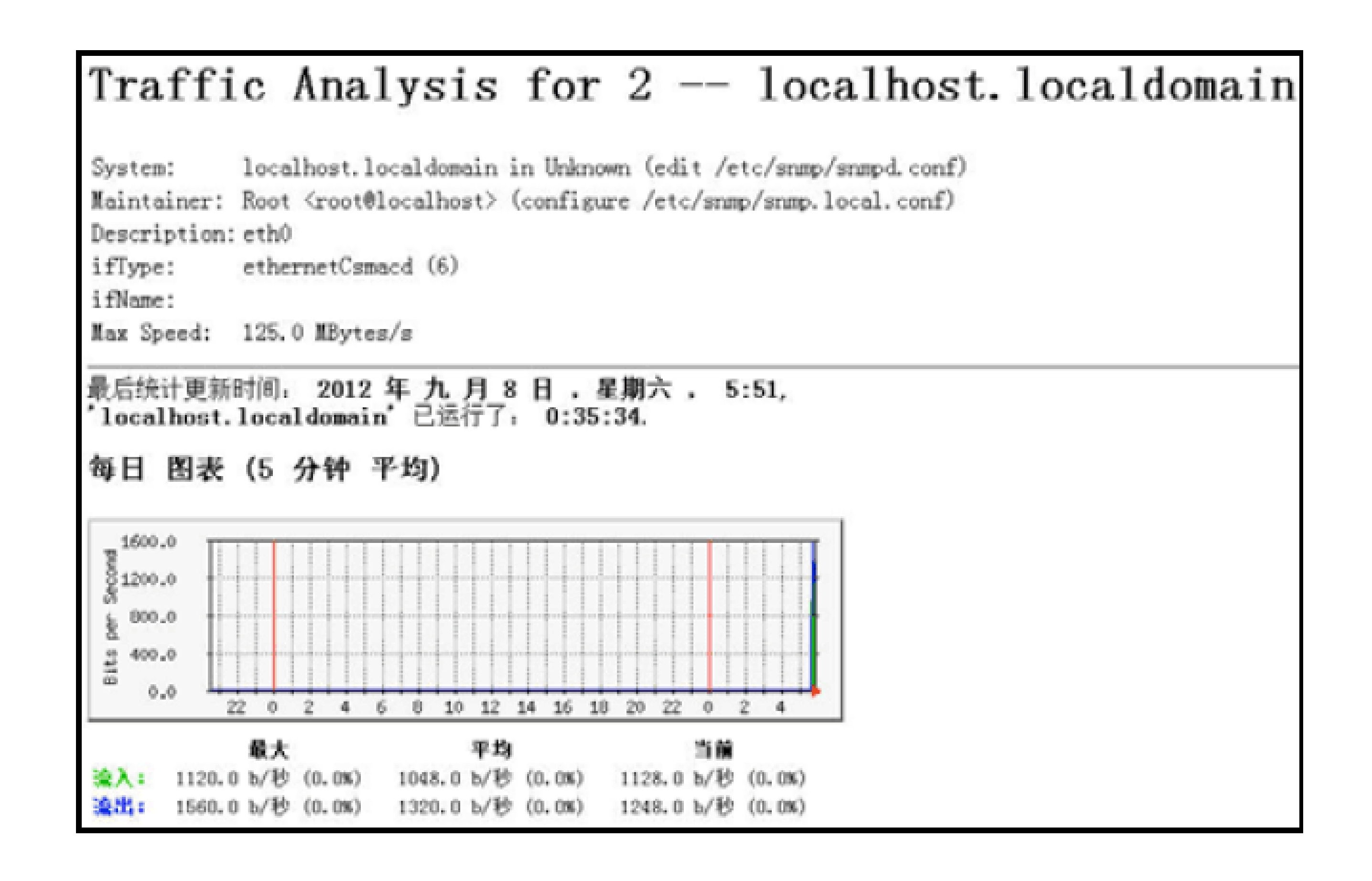
防火墙配置完毕后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                          [  OK  ]
iptables: Setting chains to policy ACCEPT: filter           [  OK  ]
iptables: Unloading modules:                                [  OK  ]
iptables: Applying firewall rules:                          [  OK  ]
```

## 浏览MRTG网页

打开浏览器，输入【http://192.168.233.10/mrtg/192.168.233.10_2.html】，如下图所示。

> **说明**
>
> 192.168.233.10为示例中MRTG服务器IP地址，请依实际环境修改。




# 24.2 MRTG分析Windows XP主机流量

MRTG不仅能检测网络设备或Linux系统，也能检测Windows平台，只要有SNMP服务都可以使用MRTG检测流量，这里检测Windows XP操作系统的网络流量。

## 示例环境介绍

下表为MRTG服务器检测客户端的相关数据。

| | |
|---|---|
| MRTG 服务器 IP 地址 | 192.168.233.10 |
| 被检测 Windows XP 客户端 IP 地址 | 192.168.233.7 |

## 在Windows XP操作系统中添加SNMP服务

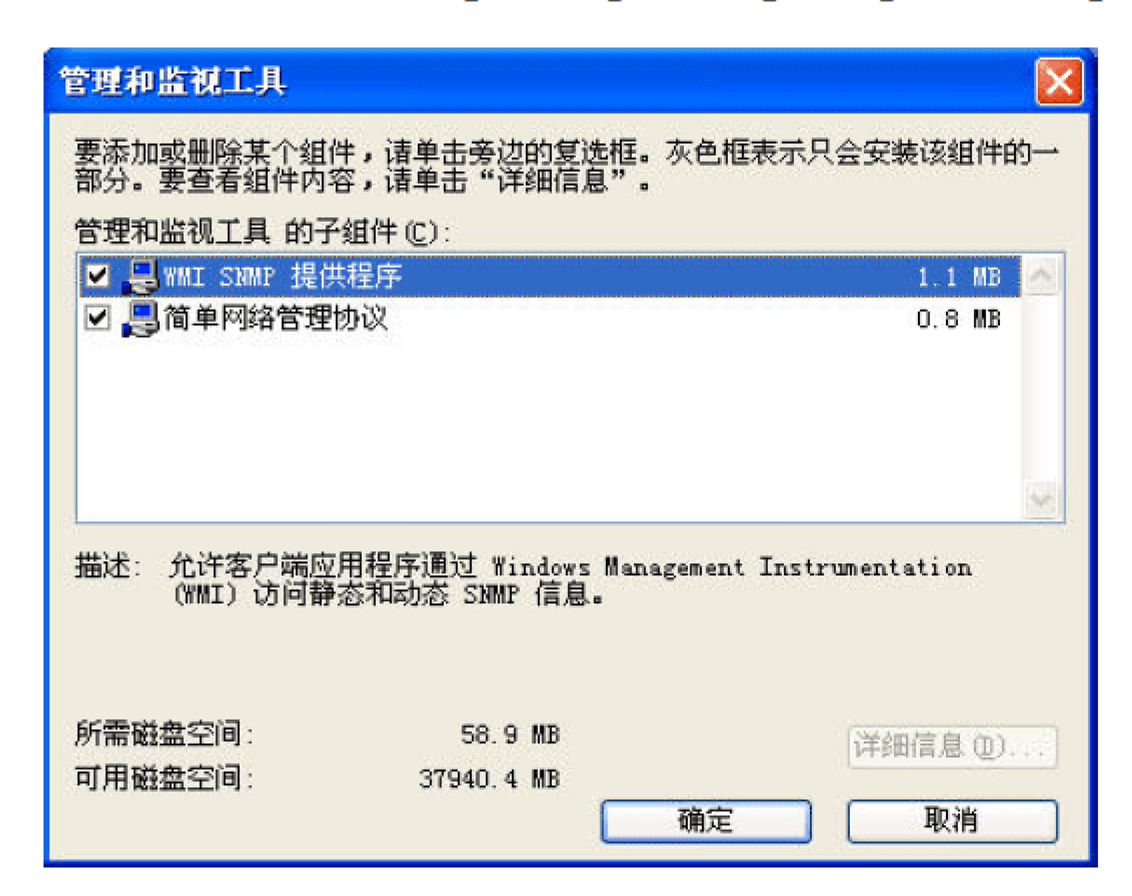
步骤 01 在Windows XP操作系统中，按【开始】→【设置】→【控制面板】→【添加或删除程序】→【添加/删除Windows组件】，安装SNMP服务。



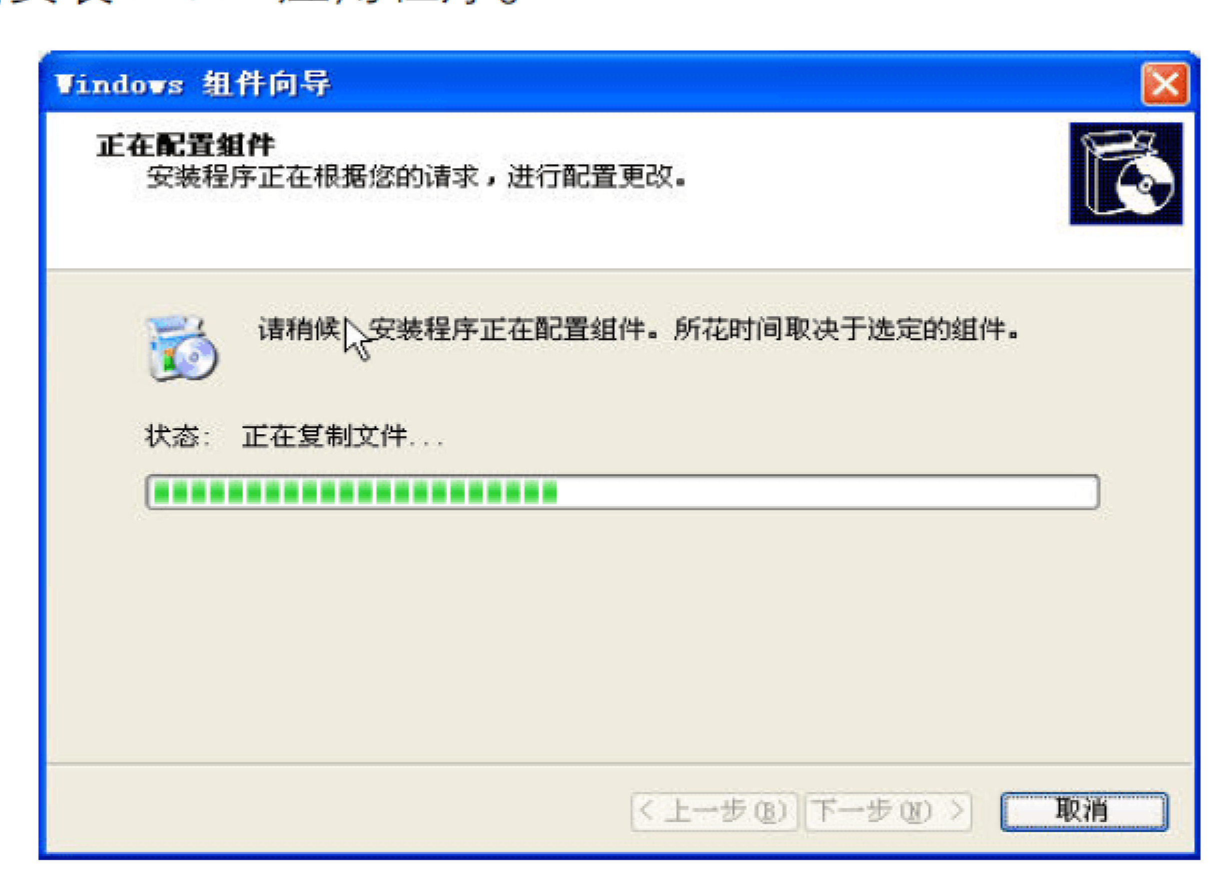
步骤02 选择【管理和监视工具】，按【详细信息】。



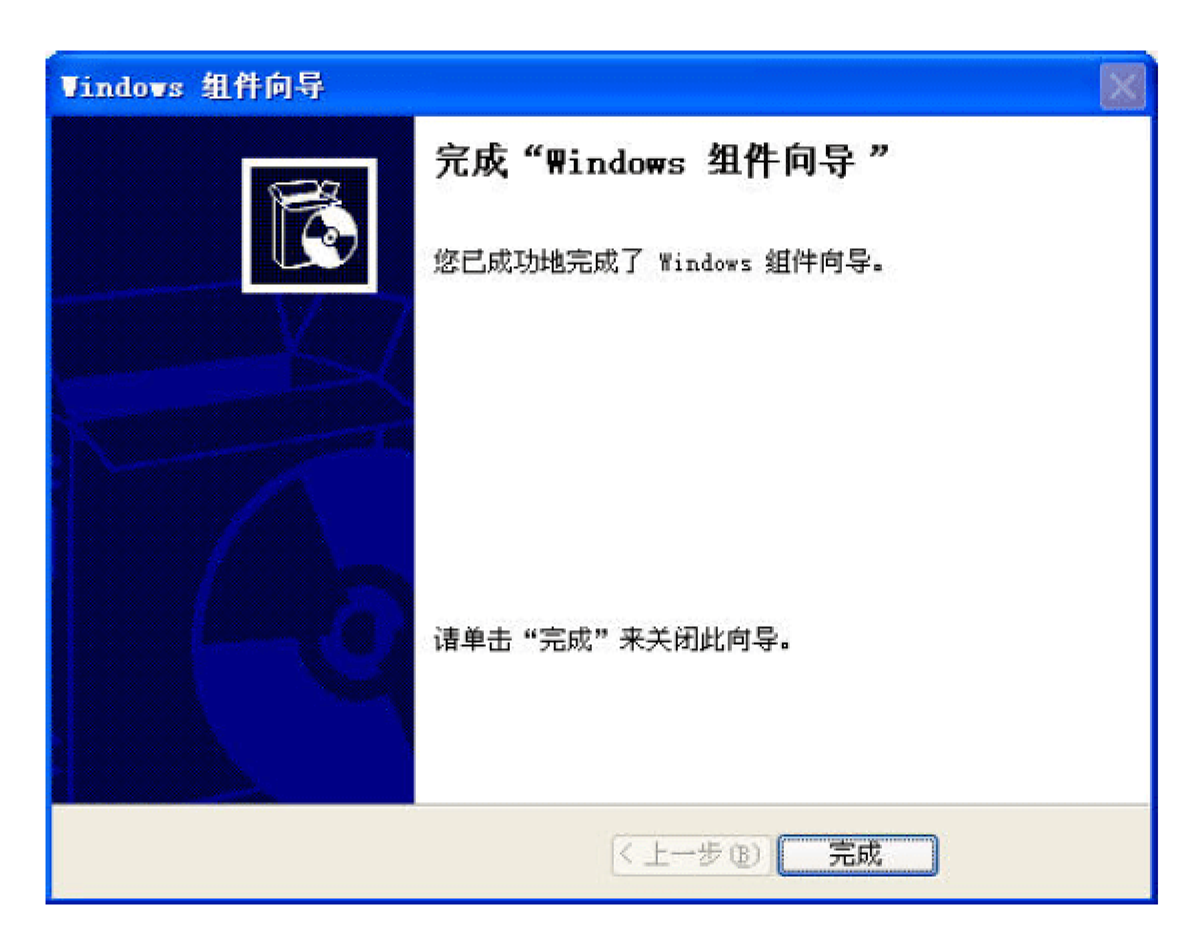

步骤03 选择【简单网络管理协议】，按【确定】和【下一步】。



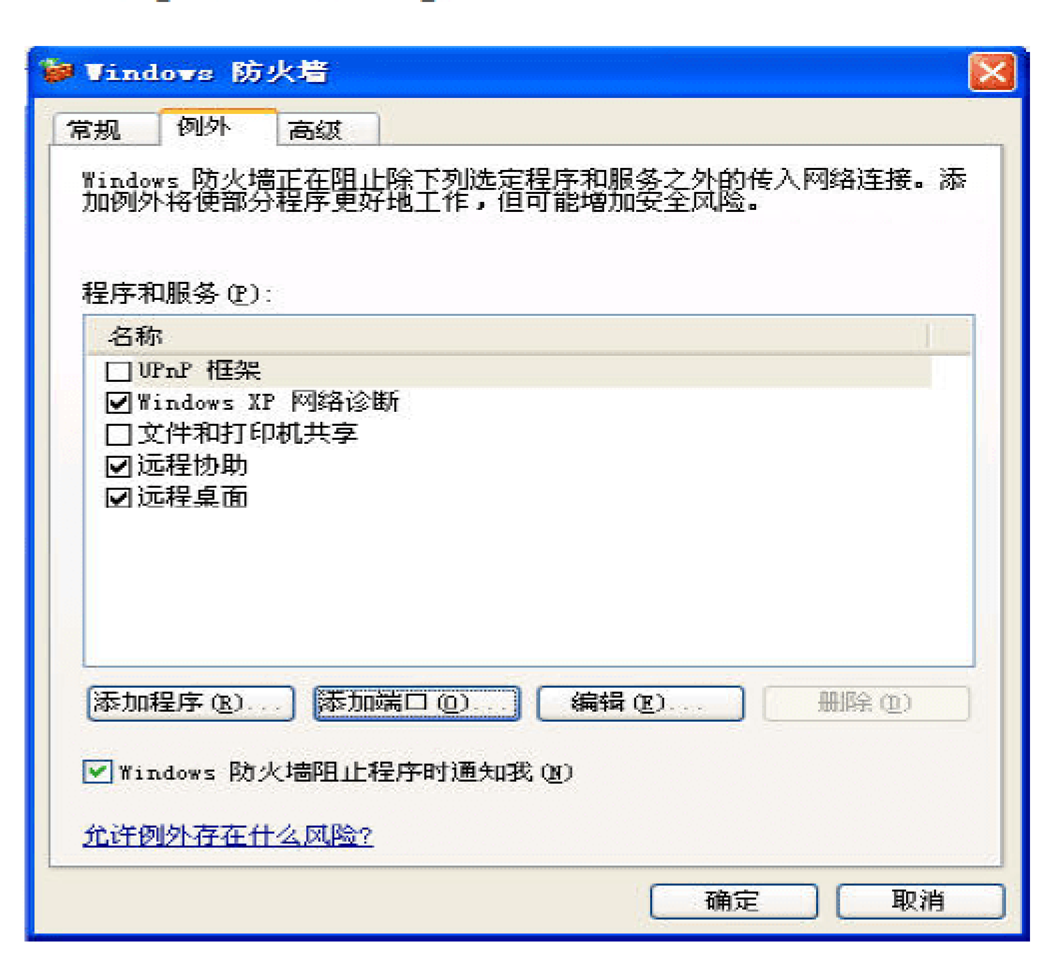

步骤04 开始安装 SNMP应用程序。



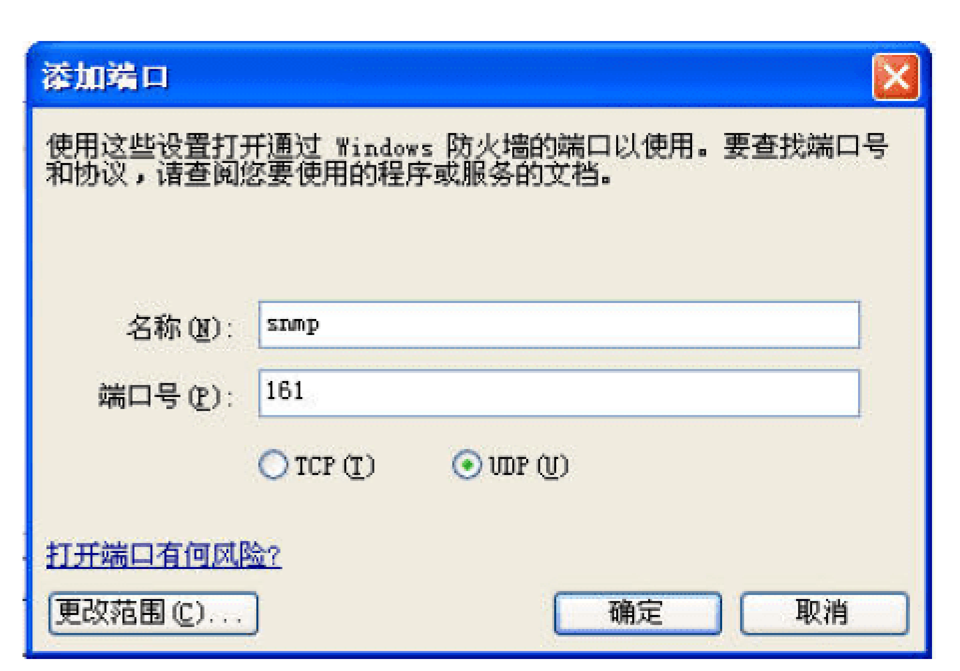

步骤05 SNMP应用程序安装完成。



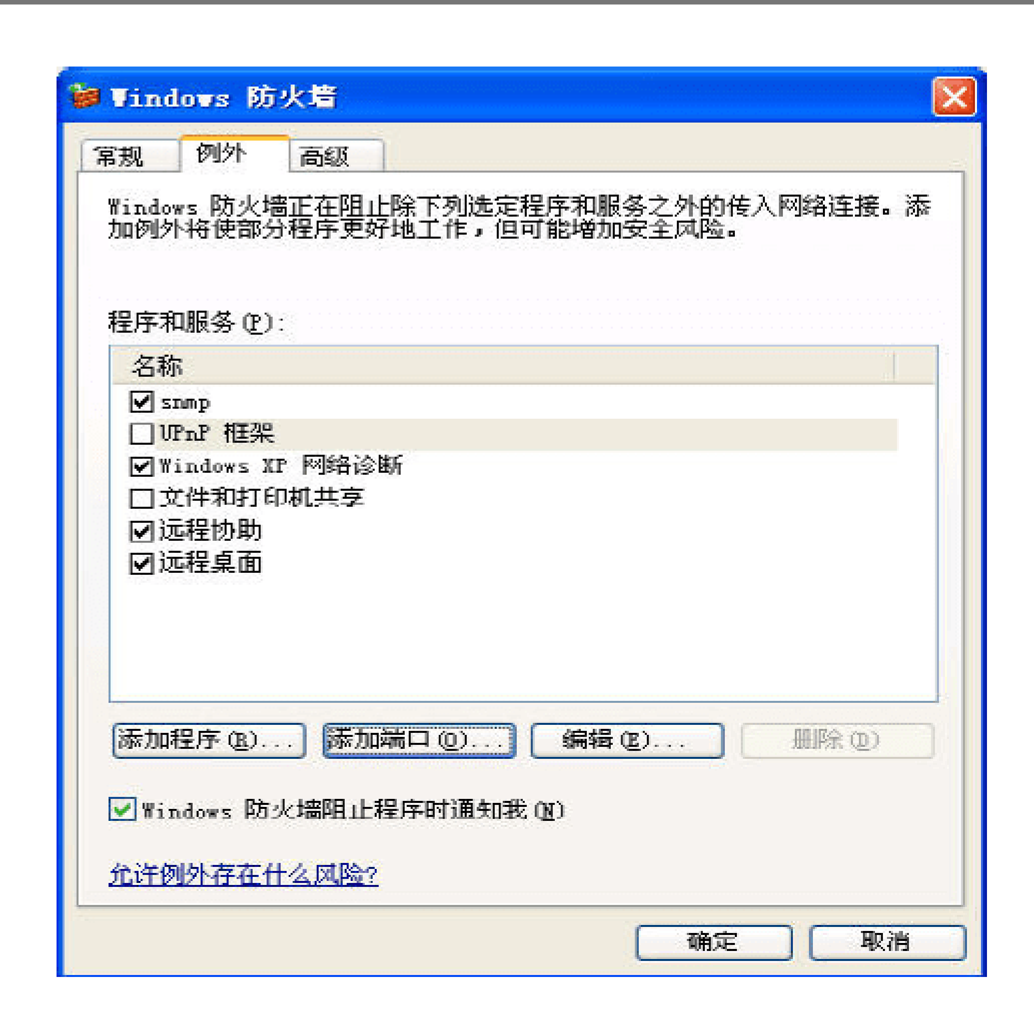

步骤06 SNMP服务安装完成后，必须开启防火墙端口，否则MRTG服务器无法检测，选择【开始】→【设置】→【控制面板】→【Windows防火墙】，选择【例外】选项卡，单击【添加端口】。




步骤07 添加SNMP的UDP 161端口，名称输入snmp（可自行配置），端口编号输入161，选择UDP，输入完毕后，按【确定】。




步骤08 添加端口成功后界面如下图所示，Windows XP部分就配置完成。




## 配置MRTG

请先行安装配置Apache、MRTG软件，相关步骤可以参考“MRTG分析统计主机流量”。

## 生成MRTG配置文件

MRTG配置完成后，就可以使用系统生成MRTG配置文件了，生成MRTG配置文件后，再编辑配置文件。

```
[root@localhost ~]# cfgmaker public@192.168.233.7 > /etc/mrtg/mrtg.cfg
                                                      //生成 MRTG 配置文件
[root@localhost ~]# vi /etc/mrtg/mrtg.cfg             //编辑 MRTG 配置文件
# Created by
# /usr/bin/cfgmaker public@192.168.233.7              //被检测的 IP 地址
### Global Config Options
#  for WINDOWS
WorkDir: /var/www/mrtg
Refresh:300
Interval:5
Language: zh_CN.UTF-8
options[_]: growright
```

## 生成MRTG网页

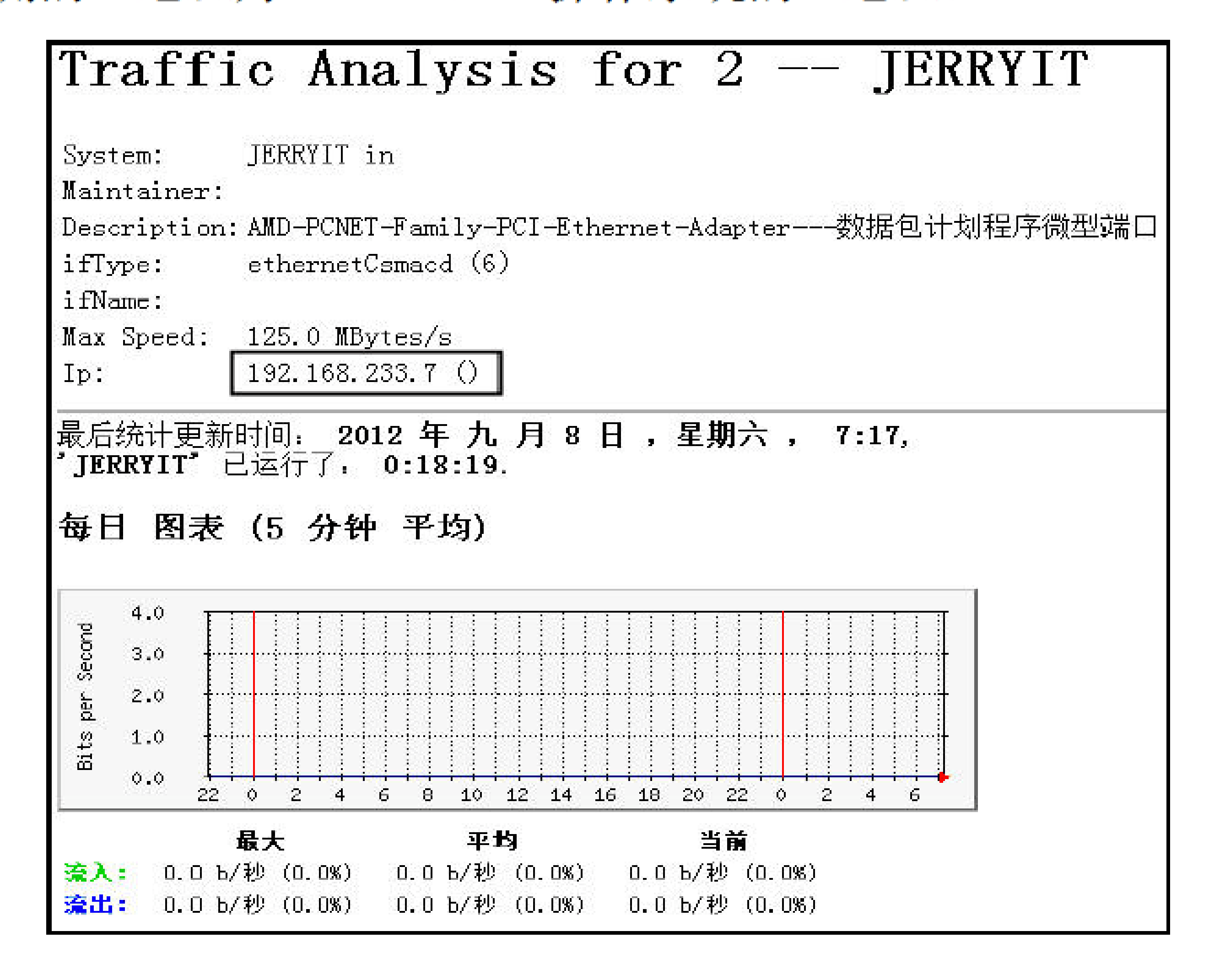
生成MRTG网页时，需要输入三次命令，到完全没有错误信息时，才算完成，若三次过后还有错误，就要检查配置文件是否有配置错误。生成MRTG网页后，记得将Apache重新启动。

```
[root@localhost ~]# env LANG=C mrtg /etc/mrtg/mrtg.cfg           //第一次
2012-09-08 19:17:20, Rateup WARNING: /usr/bin/rateup could not read the primary log file
for 192.168.233.7_2
```

```
2012-09-08 19:17:20, Rateup WARNING: /usr/bin/rateup The backup log file for
192.168.233.7_2 was invalid as well
2012-09-08 19:17:20, Rateup WARNING: /usr/bin/rateup Can't remove 192.168.233.7_2.old
updating log file
2012-09-08 19:17:20, Rateup WARNING: /usr/bin/rateup Can't rename 192.168.233.7_2.log to
192.168.233.7_2.old updating log file
[root@localhost ~]# env LANG=C mrtg /etc/mrtg/mrtg.cfg              //第二次
2012-09-08 19:17:21, Rateup WARNING: /usr/bin/rateup Can't remove 192.168.233.7_2.old
updating log file
[root@localhost ~]# env LANG=C mrtg /etc/mrtg/mrtg.cfg              //第三次
[root@localhost ~]#
```

## 打开MRTG网页

打开浏览器，输入【http://192.168.233.10/mrtg/192.168.233.7_2.html】，如下图所示，可以看到MRTG目前检测的IP地址为Windows XP操作系统的IP地址。



# 第25章

# ntop——网络流量监控工具

官方网站：http://www.ntop.org/。

ntop是一种功能类似Sniffer的网络流量监控工具。将它安装在网络上后可以显示网络的总流量，网段内各机器的流量，及各种服务所占用的流量等。甚至能列出每个节点的带宽利用率，其所显示的网络流量情况比MRTG更加详细。

## 25.1 安装ntop必备软件

在安装ntop前，必须安装一些必备软件，否则无法正常安装ntop软件，软件信息如下。

```
[root@localhost ~]# yum install -y gcc libpcap-devel libpcap  libtool  automake  autoconf
gdbm  gdbm-devel libevent libevent-devel rrdtool rrdtool-devel zlib zlib-devel
Dependencies Resolved
========================================================================
 Package    Arch  Version              Repository     Size
========================================================================
Installing:
 Autoconf      noarch   2.63-5.1.el6            base     781 k
 Automake      noarch   1.11.1-1.2.el6          base     550 k
 Gcc           x86_64   4.4.4-13.el6            base     10 M
 gdbm-deve     x86_64   1.8.0-36.el6            base     25 k
 libevent-devel x86_64 1.4.13-1.el6             base     284 k
 libpcap-develx86_64  14:1.0.0-6.20091201git117cb5.el6 base     97 k
 libtool       x86_64   2.2.6-15.5.el6          base     564 k
 rrdtool       x86_64   1.3.8-6.el6             base     293 k
 rrdtool-develx86_64   1.3.8-6.el6             base     28 k
 zlib-devel    x86_64   1.2.3-25.el6            base     43 k
Installing for dependencies:
 cloog-ppl     x86_64   0.15.7-1.2.el6          base     93 k
 cpp           x86_64   4.4.4-13.el6            base     3.7 M
 dejavu-lgc-sans-mono-fonts noarch 2.30-2.el6   base     393 k
 dejavu-sans-mono-fonts    noarch  2.30-2.el6   base     450 k
 glibc-devel   x86_64   2.12-1.7.el6_0.5        updates  961 k
```

```
 glibc-headersx86_64   2.12-1.7.el6_0.5       updates  592 k
 kernel-headers x86_64 2.6.32-71.29.1.el6     updates  991 k
 mpfr          x86_64   2.4.1-6.el6           base     157 k
 ppl           x86_64   0.10.2-11.el6         base     1.3 M
Updating for dependencies:
 Glibc         x86_64   2.12-1.7.el6_0.5      updates  3.7 M
 glibc-common x86_64   2.12-1.7.el6_0.5       updates  14 M
Transaction Summary
=========================================================================
Install      19 Package(s)
Upgrade       2 Package(s)
Total download size: 39 M
```

## 安装GeoIP

在安装ntop软件前，必须要安装GeoIP软件，由于此软件无法使用YUM在线更新安装，所以必须自行下载安装。

```
[root@localhost~]#wget http://geolite.maxmind.com/download/geoip/api/c/GeoIP.tar.gz//下载
[root@localhost ~]# tar -zxvf GeoIP.tar.gz        //解压缩 GeoIP 软件
[root@localhost ~]# cd GeoIP*                     //进入 GeoIP 安装目录
[root@localhost GeoIP-1.4.8]# ./configure         //编译安装 GeoIP 软件
…中间省略…
[root@localhost GeoIP-1.4.8]# make
…中间省略…
[root@localhost GeoIP-1.4.8]# make install
…中间省略…
```

说明

文件来源：http://geolite.maxmind.com/download/geoip/api/c/。

版本号请与实际发行版对应。

出现Zlib header（zlib.h）not found，代表zlib-devel、zlib-static没有安装。

```
checking for zlib.h... no
configure: error: Zlib header (zlib.h) not found. Tor requires zlib to build.
You may need to install a zlib development package.
```

## 下载ntop软件

所有必备软件安装完成后，接下来就是下载ntop软件，使用wget方式下载，下载完成后解压缩ntop文件。

```
[root@localhost ~]# wget
http://sourceforge.net/projects/ntop/files/ntop/Stable/ntop-4.1.0.tar.gz
                                                     //下载 ntop 软件
[root@localhost ~]# tar -zxvf ntop-4.1.0.tar.gz      //解压缩 ntop 软件
```

说明

文件来源：http://sourceforge.net/projects/ntop/files/ntop/Stable/。

版本代号请与实际发行版对应。

### 安装ntop软件

解压缩完成后，就可以安装ntop软件了，进入解压缩后的ntop程序目录，然后开始安装。

```
[root@localhost ~]# cd ntop-*                        //进入 ntop 安装目录
[root@localhost ntop-4.1.0]# ./autogen.sh            //安装 ntop
…中间省略…
[root@localhost ntop-4.1.0]# make
…中间省略…
[root@localhost ntop-4.1.0]# make install
…中间省略…
```

若没有安装GeoIP，则会出现以下错误，GeoIP无法以yum方式安装，必须要自行下载安装。

```
Removing dups and misplaced entries from LIBS and INCS...
checking for GeoIP_record_by_ipnum in -lGeoIP... no
checking for GeoIP_name_by_ipnum_v6 in -lGeoIP... no
Please install GeoIP (http://www.maxmind.com/)
```

## 25.2 创建ntop用户账号和密码

ntop软件安装完成后，需要创建ntop用户，并配置ntop目录的用户与用户组权限。

```
[root@localhost ~]# useradd -M -s /sbin/nologin -r ntop
[root@localhost ~]# chown -R ntop:root /usr/local/var/ntop/
[root@localhost ~]# chown -R ntop:ntop /usr/local/share/ntop
```

创建ntop用户密码时，需要输入两次密码，才能完成配置。

```
[root@localhost ~]# ntop -A
Fri Sep 14 23:20:30 2011  NOTE: Interface merge enabled by default
Fri Sep 14 23:20:30 2011  Initializing gdbm databases
Fri Sep 14 23:20:30 2011  Setting administrator password...
ntop startup - waiting for user response!
Please enter the password for the admin user:            //输入两次密码
Please enter the password again:
Fri Sep 14 23:20:39 2012  Admin user password has been set
Fri Sep 14 23:20:39 2012  Admin password set...
[root@localhost ~]#
```

## 配置防火墙

ntop使用的端口为3000，必须在防火墙配置文件中开启该端口，才可以对外连接。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 3000 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

修改防火墙配置后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                           [  OK  ]
iptables: Setting chains to policy ACCEPT: filter            [  OK  ]
iptables: Unloading modules:                                 [  OK  ]
iptables: Applying firewall rules:                           [  OK  ]
```

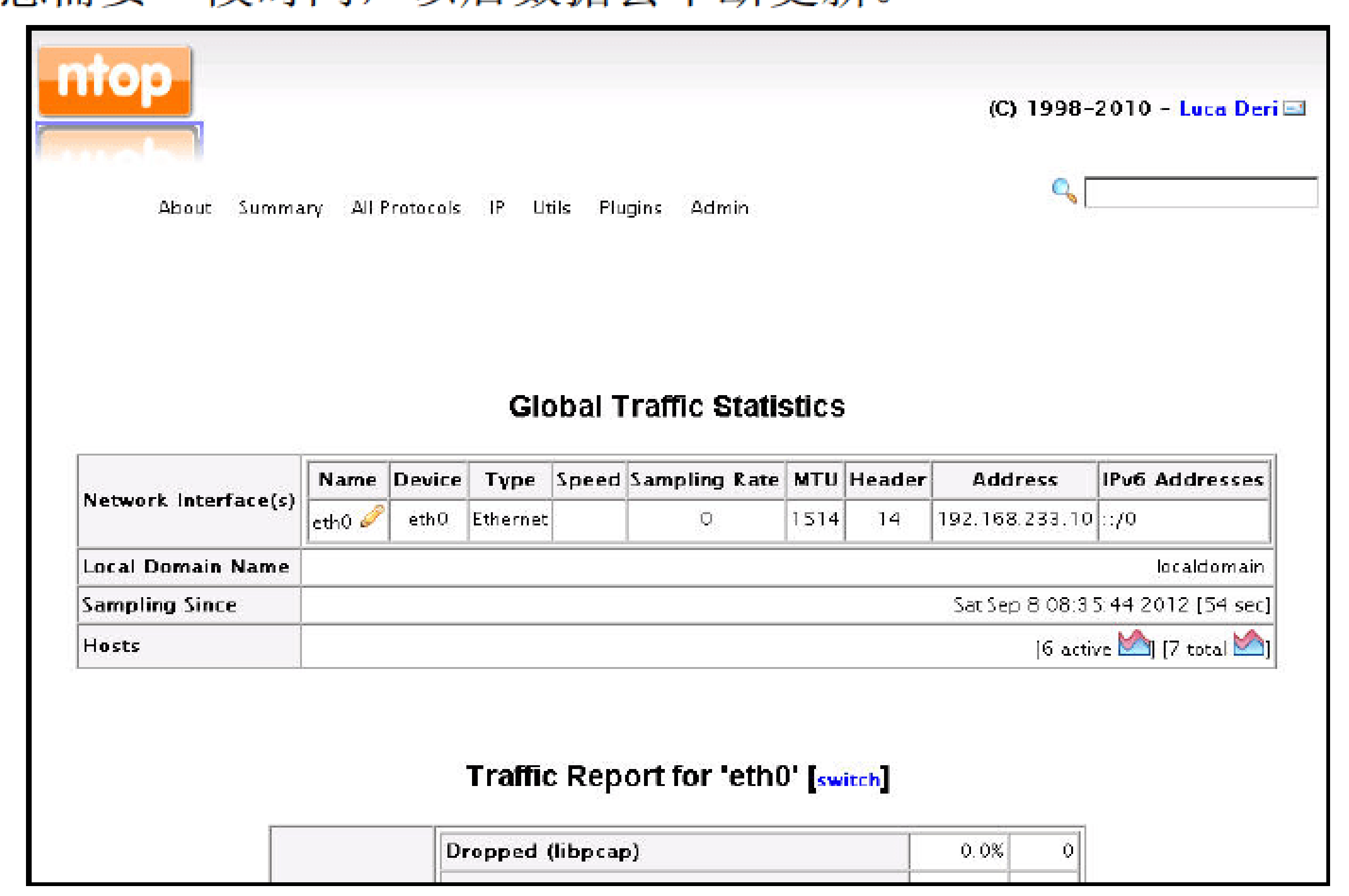
## 启动ntop服务

一切配置就绪后就可以启动ntop了，将ntop配置为默认启动，以免重新启动系统后忘记启动该服务，导致无法收集监控网络信息。

```
[root@localhost ~]# /usr/local/bin/ntop -d -L -u ntop -P /usr/local/var/ntop
--skip-version-check --use-syslog=daemon
Fri Sep 14 23:26:01 2012  NOTE: Interface merge enabled by default
Fri Sep 14 23:26:01 2012  Initializing gdbm databases
[root@localhost ~]# vi /etc/rc.local
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.
touch /var/lock/subsys/local
/usr/local/bin/ntop -d -L -u ntop -P /usr/local/var/ntop --skip-version-check
--use-syslog=daemon
```

## 25.3 测试ntop服务

打开浏览器，输入【http://IP地址:3000】，有许多选项可以查看目前环境的网络流量信息，不过收集网络信息需要一段时间，以后数据会不断更新。



# 第26章

# phpMyVisites——网站流量统计系统

phpMyVisites官方网站：http://www.phpmyvisites.us/。

phpMyVisites是一款免费的网站流量统计系统，支持多国语言，统计的数据包含许多方面，功能强大，不方便的地方是要在每处都使用JavaScript才可以统计，有点儿美中不足，不过这款软件本身还是相当棒的。

phpMyVisites官方Demo网站：http://www.phpmyvisites.us/phpmv2/。

刚创建好的phpMyVisites系统没任何数据，因为统计网络流量需要一定的时间，为了熟悉phpMyVisites系统的各项功能，可以先到官方的Demo网站查看。

下面介绍如何安装和配置phpMyVisites服务，然后利用检测到的数据，生成网站的统计数据。

## 26.1 安装必备软件

为了能够正常使用phpMyVisites服务，必须安装Apache、php、php-mysql、php-gd、freetype软件可以使用yum在线更新方法安装。

```
[root@localhost ~]# yum install  -y httpd php-mysql  php-gd  freetype
Dependencies Resolved
=======================================================================
 Package       Arch  Version        Repository       Size
=======================================================================
Installing:
 Httpd          x86_64   2.2.15-5.el6.centos base     811 k
 php-gd         x86_64   5.3.2-6.el6_0.1     updates  103 k
 php-mysql      x86_64   5.3.2-6.el6_0.1     updates  75 k
Updating:
 Freetype       x86_64   2.3.11-6.el6_0.2    updates  359 k
Installing for dependencies:
 apr            x86_64   1.3.9-3.el6_0.1     updates  124 k
 apr-util       x86_64   1.3.9-3.el6_0.1     updates  87 k
 apr-util-ldap  x86_64   1.3.9-3.el6_0.1     updates  15 k
```

```
 httpd-tools     x86_64   2.2.15-5.el6.centos  base     68 k
 libXpm          x86_64   3.5.8-2.el6          base     59 k
 php-common      x86_64   5.3.2-6.el6_0.1      updates  516 k
 php-pdo         x86_64   5.3.2-6.el6_0.1      updates   72 k
Transaction Summary
========================================================================
Install      10 Package(s)
Upgrade       1 Package(s)
Total download size: 2.2 M
```

## 下载并安装phpMyVisites服务

使用wget命令下载phpmyvisites压缩文件进行安装，安装办法十分简单，如下所示，将phpmyvisites文件解压缩，解压缩后的目录名称为phpmv2，将phpmv2复制到Apache网页主目录，并将phpmv2重命名为phpmv。

```
[root@localhost ~]# wget http://www.phpmyvisites.us/phpmyvisites_2_4.zip
                                                 //下载 phpmyvisites 安装文件
…中间省略…
[root@localhost ~]# unzip phpmyvisites_2_4.zip   //解压缩 phpmyvisites
…中间省略…
[root@localhost ~]# mv phpmv2 /var/www/html/phpmv   //复制目录并重命名
```

## 启动Apache 服务

Apache网页服务器安装完成后，需要启动Apache服务，这样才可以安装phpMyVisites。为了方便提供phpMyVisites服务，请将Apache配置为默认启动。

```
[root@localhost ~]# service httpd start
Starting httpd:                                            [  OK  ]
[root@localhost ~]# chkconfig httpd on
```

## 配置防火墙

phpMyVisites系统用到了Apache服务，所以必须在防火墙配置中开启80端口，这样才可以对外连接。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
```

```
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                      [  OK  ]
iptables: Setting chains to policy ACCEPT: filter       [  OK  ]
iptables: Unloading modules:                            [  OK  ]
iptables: Applying firewall rules:                      [  OK  ]
```

### 创建数据库

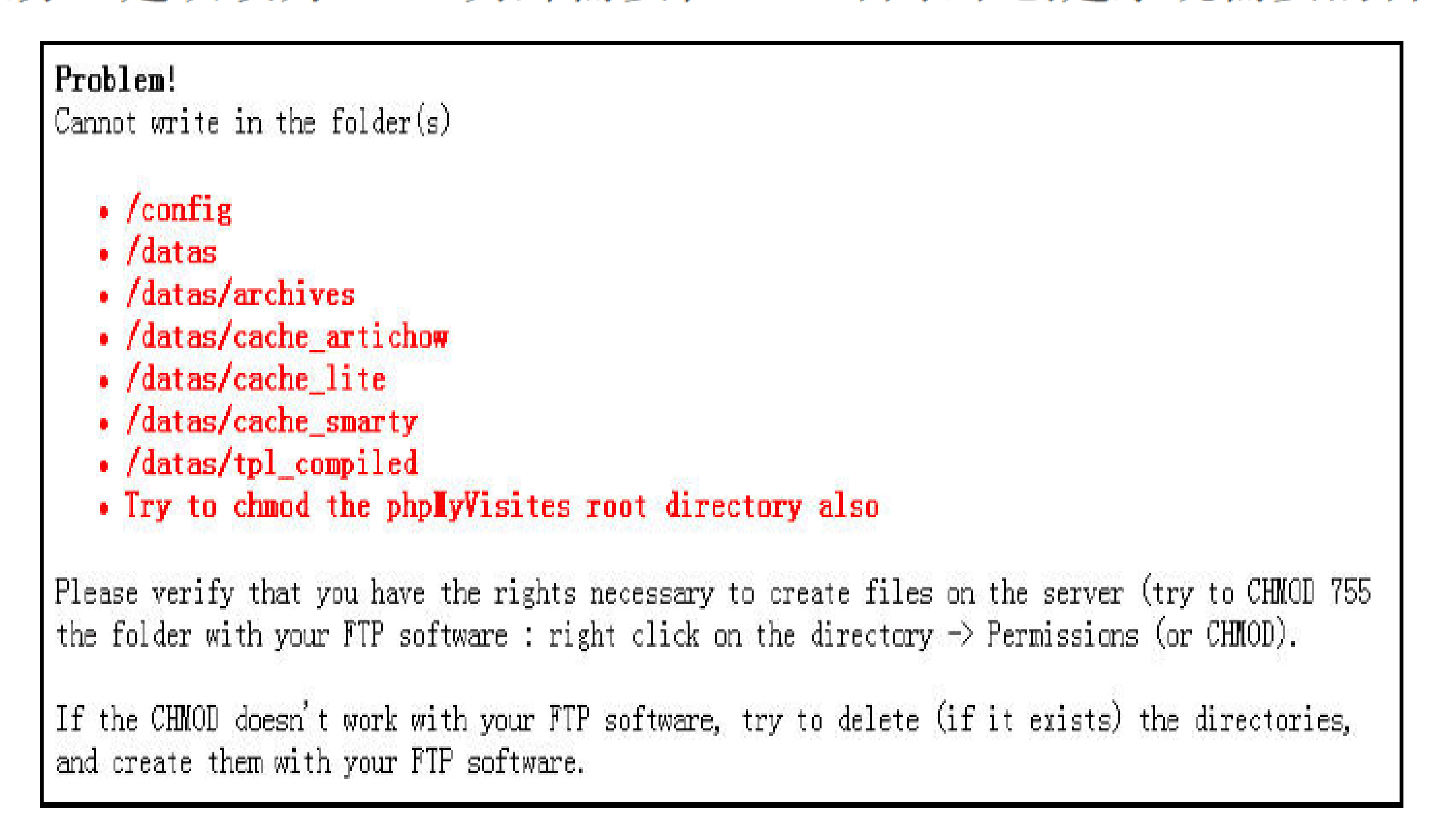
创建一个提供phpMyVisites的数据库，数据库名称为phpmv。有关如何安装MySQL请参考MySQL相关配置，这里不再多说。

```
[root@localhost ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.1.52 Source distribution
Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> create database phpmv;         //创建 phpmv 数据库
Query OK, 1 row affected (0.00 sec)
mysql> show databases;          //查看所有数据库
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| phpmv              |
| test               |
+--------------------+
4 rows in set (0.00 sec)
mysql> quit               //退出 MySQL 服务
Bye
```

## 26.2 安装并配置phpMyVisites 服务

打开浏览器前请先将SELinux关闭。在浏览器中输入【http://IP或网址/phpmv】，会提示

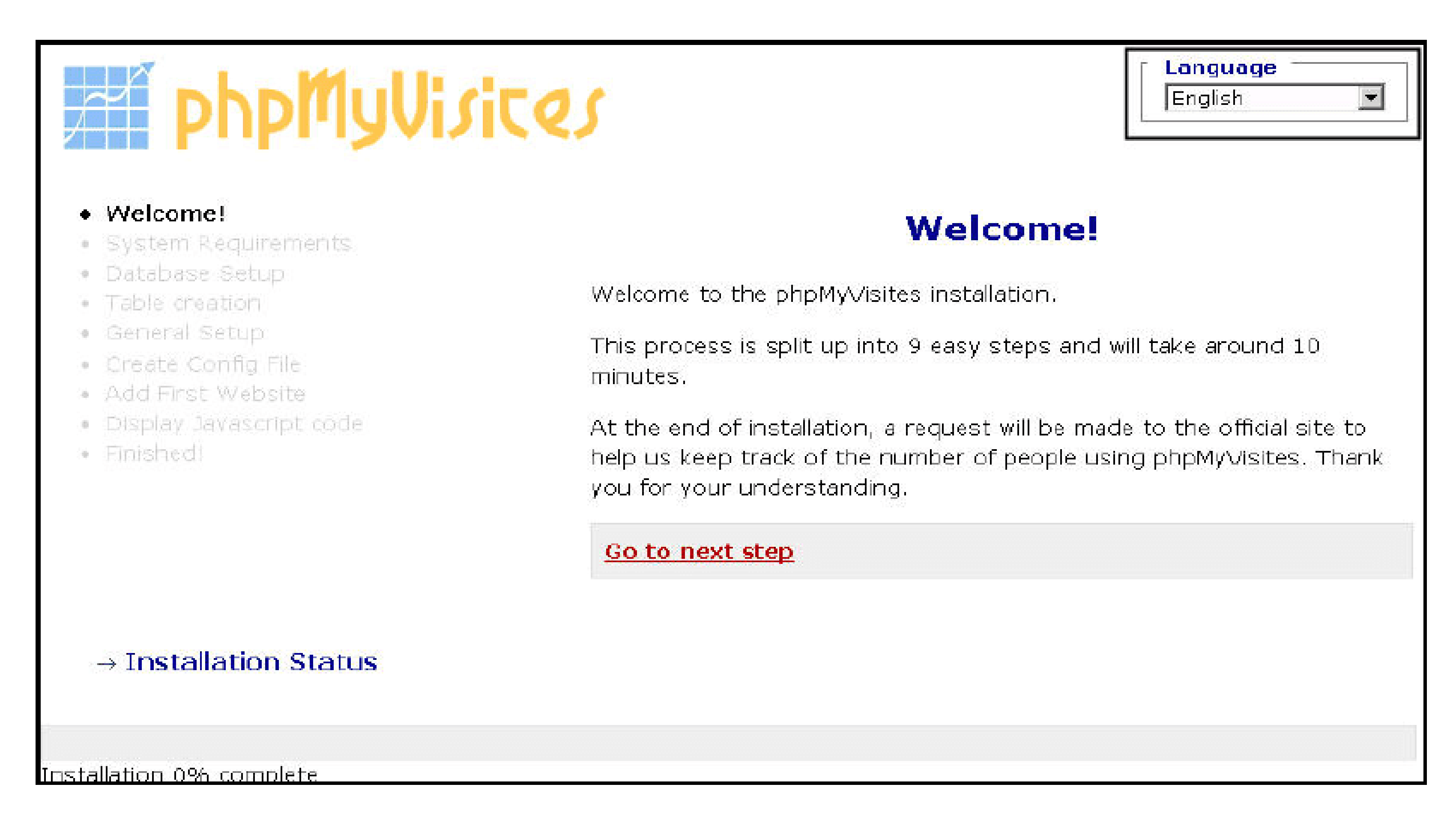
phpmv安装文件需要配置权限，显示信息提示文件权限配置为755，为了能够正常安装phpMyVisites 服务，建议设为777，另外需要在/datas目录下创建系统需要的目录。




进入phpmv目录，在datas目录下创建archives、cache_artichow、cache_lite、cache_smarty、tpl_compiled目录，然后将datas及config目录权限配置为777，重新整理后，刷新浏览器，就不会有警告信息，而是显示phpMyVisites安装画面。

```
[root@localhost ~]# cd /var/www/html/phpmv
[root@localhost phpmv]# mkdir datas/archives datas/cache_artichow datas/cache_lite
datas/cache_smarty datas/tpl_compiled
[root@localhost phpmv]# chmod 777 config | chmod 777 -R datas
```

选择语言，默认为English，若要使用简体中文，选择【Simplified Chinese】。




简体中文安装向导欢迎界面如下所示，通过9个步骤依序安装即可，按【下一步】。




检查系统环境，如果成功，如下图所示，按【下一步】。

系统环境

→需求

| | |
|---|---|
| PHP version > 4.3 | ✔ |
| Mysql extension | ✔ |
| PHP-XML extension (utf8_decode function) | ✔ |
| 目录可写 | ✔ /config<br>✔ /datas<br>✔ /datas/archives<br>✔ /datas/cache_artichow<br>✔ /datas/cache_lite<br>✔ /datas/cache_smarty<br>✔ /datas/tpl_compiled |

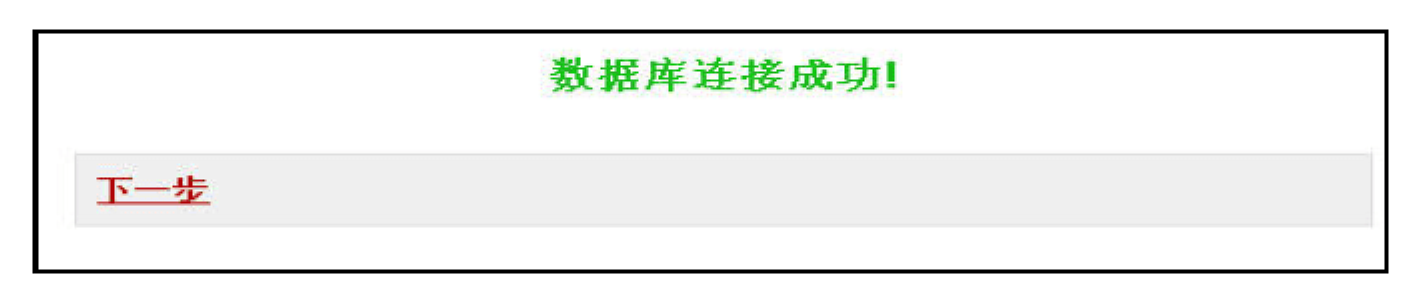
配置数据库，输入数据库相关信息，这里可以使用已创建的phpmv数据库，输入完成后，按【提交】。



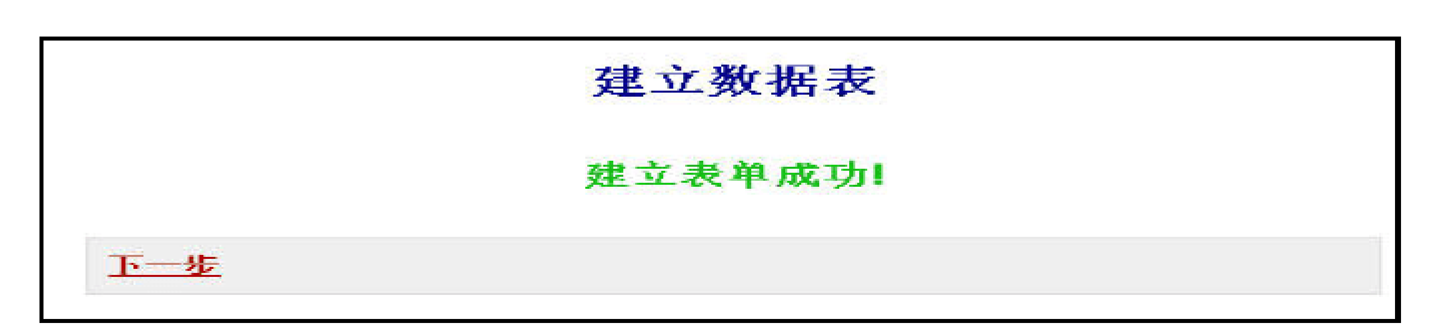
**说明**

phpMyVisites服务与MySQL服务如果在同一台服务器上，则输入localhost，如果不是请输入数据库服务器IP地址。

如果数据库连接失败，就不能正常进行下一步的操作了，如果数据库连接成功，如下图所示，按【下一步】。




数据库连接成功后，就会创建系统所使用的数据表，创建数据表成功信息如下图所示，按【下一步】。如果数据表创建失败，则无法继续下一步的操作。




在【管理配置】中会创建超级管理员（最大权限）账号、密码及电子邮箱，如下图所示。

管理配置

phpMyVisites 仅提供一个拥有全部权限的超级管理员，请输入该管理员的用户名及密码，此后您可以添加其他不同权限的用户。

→ General - phpMyVisites

超级管理员帐号: jerry
超级管理员密码: •••••••
确认密码: •••••••
超级管理员Email jerry@jerryit.idv.cn
每日接收各站点统计Email? 是 / 否
每周开始时间 星期一 / 星期日

程序的完整访问路径是Apache网页主目录下的phpMyVisites程序目录，如果有真实的网址，请修改网址信息，如果没有，暂时使用IP地址，默认语言不变，设为【Simplified Chinese】，按【提交】。

程序的完整访问路径 http://192.168.233.10/phpmv
默认语言?
也作为Email的默认语言 Simplified Chinese
提交

管理员信息配置成功后，会出现如下信息，按【下一步】。

管理员信息输入成功

下一步

对于高级选项，可以使用默认配置，按【提交】。

→ 高级选项(可选)

记录变量？（url变量） ◉ 记录所有url变量 ○ 不记录url变量 ○ 记录指定变量 ○ 记录除指定外变量

变量名（; 独立列表） 例如：*id;data;page*

PDF报告: 默认PDF报告

用户可视界面: Default

提交

成功创建站点后，按【下一步】。

成功建立站点!

下一步

若想统计所有的访问量，必须将以下JavaScript代码插入到所要统计的网页中！网页不一定要使用PHP语言编程，phpMyVisites适用于所有的网页语言（如HTML、ASP、Perl等语言），按【下一步】。



**显示javascript调用代码**

要实现网站统计，您需要将javascript代码插入到要统计的页面中。

您的网站不一定要使用PHP语言编写，**phpMyVisites 适用于所有的网页语言（包括 HTML，ASP，Perl 等语言）。**

以下是您需要插入页面的代码：(复制并粘贴在您的页面中)。

```
<!-- phpmyvisites -->
<a href="http://www.phpmyvisites.us/" title="phpMyVisites 免费的网站统
计、流量分析软件"
onclick="window.open(this.href);return(false);"><script
type="text/javascript">
<!--
var a_vars = Array();
var pagename='';

var phpmyvisitesSite = 1;
var phpmyvisitesURL =
"http://192.168.233.10/phpmv/phpmyvisites.php";
//-->
</script>
<script language="javascript"
src="http://192.168.233.10/phpmv/phpmyvisites.js"
type="text/javascript"></script>
<object><noscript><p>phpMyVisites 免费的网站统计、流量分析软件
<img src="http://192.168.233.10/phpmv/phpmyvisites.php"
alt="Statistics" style="border:0" />
</p></noscript></object></a>
<!-- /phpmyvisites -->
```

phpMyVisites安装成功后，单击【进入phpMyVisites!】，进入网站。

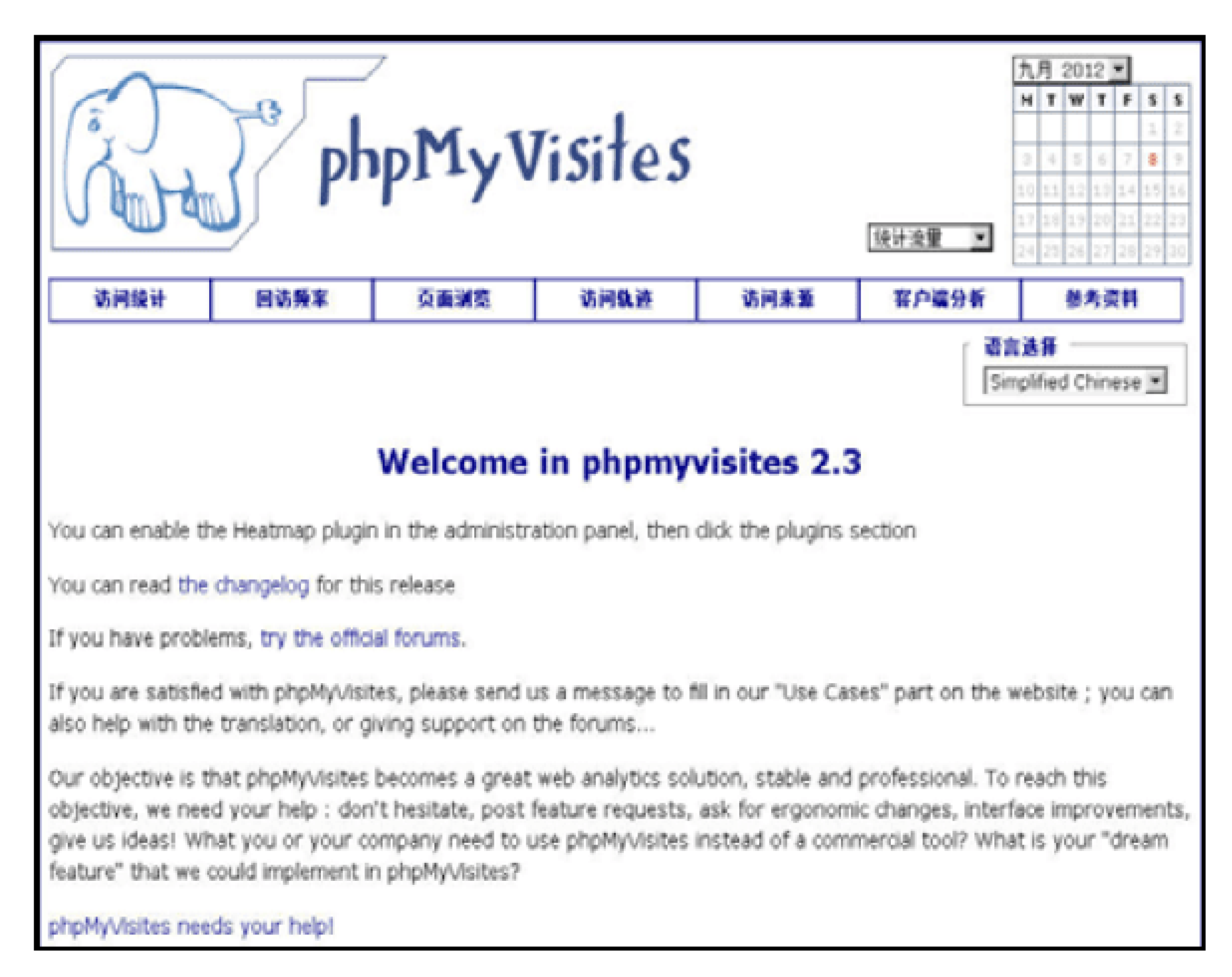



## 26.3 浏览phpMyVisites网站

进入phpMyVisites网站前，必须要输入超级管理员账号和密码才可以登录。




登录phpMyVisites统计网站后，显示如下信息，刚开始浏览时没有任何数据。




进入phpMyVisites系统管理页面，可以进行系统配置，如下图所示。




## 将JavaScript代码添加到网页进行统计

将JavaScript代码添加到个人网页，在【系统管理】页面中按下【显示 JavaScript 统计代码】，会出现下图所示的信息。

回到统计页面

Site selected for administration : www.jerryit.idv.cn (id = 1)

**显示javascript调用代码**

要实现网站统计，您需要将javascript代码插入到要统计的页面中。

您的网站不一定要使用PHP语言编写，phpMyVisites 适用于所有的网页语言（包括 HTML，ASP，Perl 等语言）。

以下是您需要插入页面的代码：(复制并粘贴在您的页面中)。

```
<!-- phpmyvisites -->
<a href="http://www.phpmyvisites.us/" title="phpMyVisites 免费的网站统计，流量分析软件"
onclick="window.open(this.href);return(false);"><script type="text/javascript">
<!--
var a_vars = Array();
var pagename='';

var phpmyvisitesSite = 1;
var phpmyvisitesURL = "http://192.168.233.10/phpmv/phpmyvisites.php";
//-->
</script>
<script language="javascript" src="http://192.168.233.10/phpmv/phpmyvisites.js" type="text/javascript"></script>
<object><noscript><p>phpMyVisites 免费的网站统计，流量分析软件
<img src="http://192.168.233.10/phpmv/phpmyvisites.php" alt="Statistics" style="border:0" />
</p></noscript></object></a>
<!-- /phpmyvisites -->
```

在/var/www/html目录下创建index.htm网页，将以下内容输入到index.htm网页里，输入完成后保存退出。

```
[root@localhost ~]# vi /var/www/html/index.htm
<!-- phpmyvisites -->
<a href="http://www.phpmyvisites.us/" title="phpMyVisites | 开放源代码的网站流量统计软件"
onclick="window.open(this.href);return(false);"><script type="text/javascript">
<!--
var a_vars = Array();
var pagename='';
var phpmyvisitesSite = 1;
var phpmyvisitesURL = "http://192.168.233.10/phpmv/phpmyvisites.php";
//-->
</script>
```

```
<script language="javascript" src="http://192.168.233.10/phpmv/phpmyvisites.js"
type="text/javascript"></script>
<object><noscript><p>phpMyVisites | 开放源代码的网站流量统计软件
<img src="http://192.168.233.10/phpmv/phpmyvisites.php" alt="Statistics"
style="border:0" />
</p></noscript></object></a>
<!-- /phpmyvisites -->
```

打开浏览器，输入【http://IP地址/index.htm】，画面如下图所示。




再去phpMyVisites系统查看统计报告，就会开始有统计数据，如下图所示。




**说明**

网站页面都要添加JavaScript代码，才会统计所有页面。

# 第27章

# Webalizer——日志文件分析工具

Webalizer官方网站：http://www.mrunix.net/webalizer/。

Webalizer是一款高效的、免费的Web Server日志文件分析软件，它除了能够分析 Apache Web Server 所产生的log日志文件之外，还能够分析FTP 的 Log日志，并以相当精美的HTML网页输出，目前许多网站都使用这一款软件作为网站日志分析工具。

Webalizer官方下载：http://www.mrunix.net/webalizer/download.html。

Webalizer可以使用YUM方式安装。

## 27.1 安装Webalizer

### 安装Webalizer软件

使用Webalizer软件需要httpd的支持，可使用YUM在线更新方式安装所有软件。

```
[root@localhost ~]# yum install -y webalizer httpd
Dependencies Resolved
========================================================================
 Package            Arch         Version                 Repository       Size
========================================================================
Installing:
 httpd               x86_64       2.2.15-5.el6.centos     base            811 k
 webalizer           x86_64       2.21_02-3.3.el6         base            128 k
Installing for dependencies:
 apr                 x86_64       1.3.9-3.el6_0.1         updates         124 k
 apr-util            x86_64       1.3.9-3.el6_0.1         updates          87 k
 apr-util-ldap       x86_64       1.3.9-3.el6_0.1         updates          15 k
 gd                  x86_64       2.0.35-10.el6           base            142 k
 httpd-tools         x86_64       2.2.15-5.el6.centos     base             68 k
 libXpm              x86_64       3.5.8-2.el6             base             59 k
Transaction Summary
```

```
================================================================================
Install       8 Package(s)
Upgrade       0 Package(s)
Total download size: 1.4 M
```

## 配置Webalizer

编辑Webalizer配置文件，例如连接允许Webalizer服务的IP地址是192.168.233.100，如果要全部都允许连接，只要将Deny from all参数改成Allow from all参数，就可以让所有用户连接，不过建议配置单一用户，这样可保证Webalizer服务的安全。

```
[root@localhost ~]# vi /etc/httpd/conf.d/webalizer.conf
# This configuration file maps the webalizer log analysis
# results (generated daily) into the URL space.  By default
# these results are only accessible from the local host.
Alias /usage /var/www/usage

<Location /usage>
    Order deny,allow
#   Deny from all
    Allow from 192.168.233.100/255.255.255.0
    Allow from 127.0.0.1
    Allow from ::1
    # Allow from .example.com
</Location>
```

## 配置防火墙

Webalizer服务需要Apache服务的支持，所以需要在防火墙配置中开启80端口，这样才可以对外连接。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

### 启动Apache 服务

一切配置完成后，就可以启动Apache服务了。将Apache配置为系统默认启动。

```
[root@localhost ~]# service httpd start
Starting httpd:                                            [  OK  ]
[root@localhost ~]# chkconfig httpd on
```

### 生成Webalizer日志文件

生成Webalizer日志文件，第一次浏览webalizer服务没有任何信息，建议执行两次webalizer命令，因为有时执行一次也没有画面。

```
[root@localhost ~]# /usr/bin/webalizer
No valid records found!
[root@localhost ~]# /usr/bin/webalizer
```

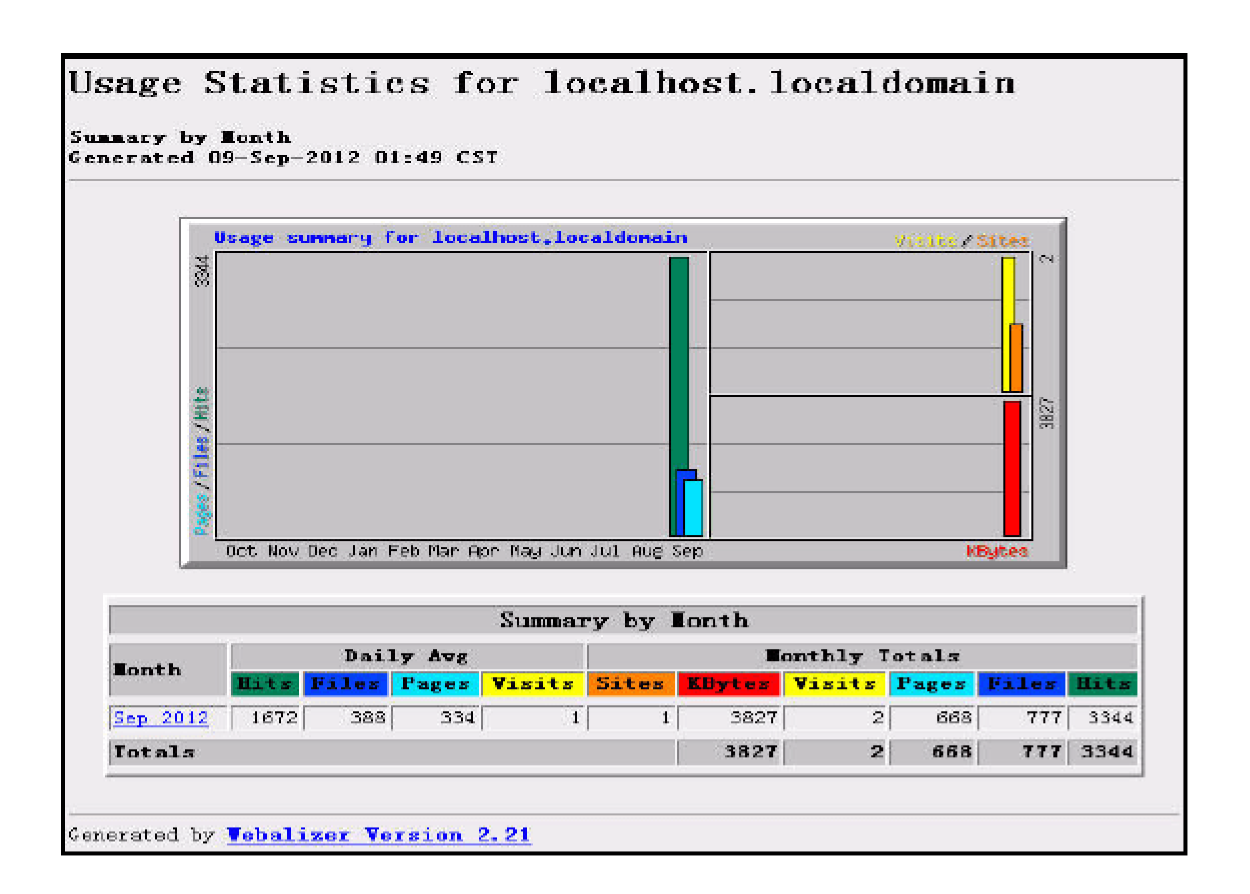
### 利用cron生成日志文件

使用计划任务生成日志文件，例如配置每30分钟生成一次数据。

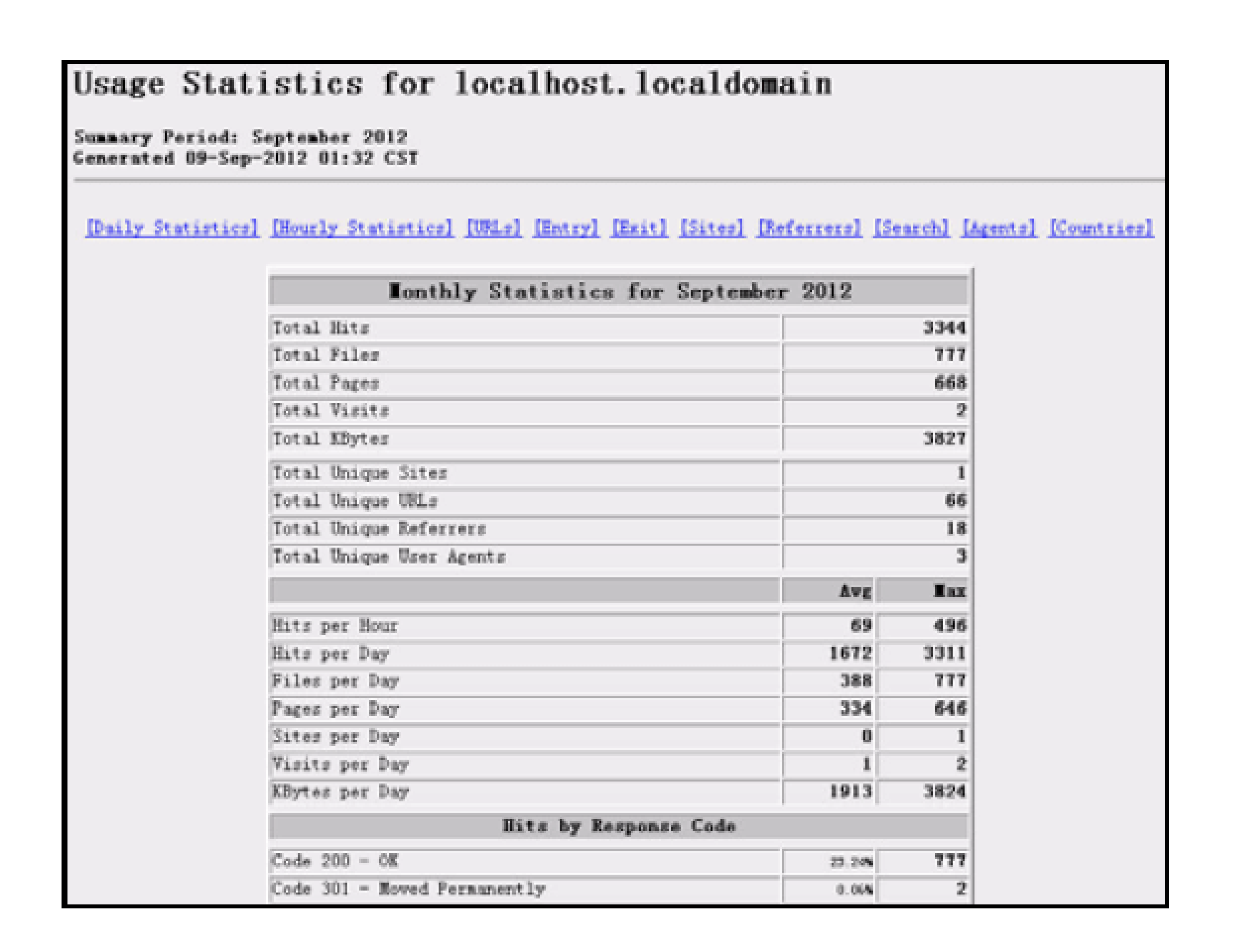
```
[root@localhost ~]# crontab -e
*/30 * * * *     root          /usr/bin/webalizer
```

## 27.2 测试Webalizer服务

在浏览器中输入【http://IP或网址/usage/】，浏览画面如下图所示，有图表，也有数据。


Usage Statistics for localhost.localdomain
Summary by Month
Generated 09-Sep-2012 01:49 CST
Usage summary for localhost.localdomain
Visits / Sites
3344
Pages / Files / Hits
2
3827
Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep
KBytes
Summary by Month
Month
Daily Avg
Monthly Totals
Hits Files Pages Visits Sites KBytes Visits Pages Files Hits
Sep 2012 1672 388 334 1 1 3827 2 668 777 3344
Totals 3827 2 668 777 3344
Generated by Webalizer Version 2.21

统计数据：


Usage Statistics for localhost.localdomain
Summary Period: September 2012
Generated 09-Sep-2012 01:32 CST
[Daily Statistics] [Hourly Statistics] [URLs] [Entry] [Exit] [Sites] [Referrers] [Search] [Agents] [Countries]
Monthly Statistics for September 2012
Total Hits 3344
Total Files 777
Total Pages 668
Total Visits 2
Total KBytes 3827
Total Unique Sites 1
Total Unique URLs 66
Total Unique Referrers 18
Total Unique User Agents 3
Avg Max
Hits per Hour 69 496
Hits per Day 1672 3311
Files per Day 388 777
Pages per Day 334 646
Sites per Day 0 1
Visits per Day 1 2
KBytes per Day 1913 3824
Hits by Response Code
Code 200 - OK 777
Code 301 - Moved Permanently 2

# 第五部分

# LAMP配置篇

# 第28章

# LAMP——创建网站基本需求软件

LAMP是目前CentOS操作系统创建网站的基本需求软件，网站网页程序都以PHP语言开发，创建网站的方法大同小异，都以LAMP为主。所谓LAMP是一个缩写，是指Linux操作系统、Apache网页服务器、MySQL数据库、PHP网页编程语言所组成，在Windows操作系统中，LAMP中的L其实可以是W，W就是Windows不过在此不做介绍。此章节所介绍的网站创建软件，都必须要先配置好LAMP环境，否则无法进行安装。

## LAMP系统需求

LAMP环境是创建网站的基本需求，配置前请先确认是否符合所有要求。

| 基本需求 | 软件名称 |
|---|---|
| 操作系统 | CentOS 6.x |
| 创建网站 | Apache 2（httpd） |
| 数据库 | MySQL 5 |
| 网页支持语言 | PHP 5 |

## 28.1 安装Apache、MySQL、PHP软件

Apache、MySQL、PHP服务运行在CentOS操作系统上，所以一定要先安装CentOS操作系统，要安装的软件详细资料，如下表所示。

| | |
|---|---|
| Apache 网站配置 | httpd |
| MySQL 数据库 | mysql<br>mysql-server |
| PHP 网页语言 | php<br>php-mbstring 字符集编码<br>php-gd 图形识别码<br>php-mysql 连接 MySQL 数据库 |

首先安装Apache、MySQL、PHP软件，确认所有软件都已安装，否则以后配置软件会失败。

```
[root@localhost ~]# yum install -y httpd  mysql mysql-server php php-mbstring  php-gd
php-mysql
Dependencies Resolved
========================================================================
 Package            Arch       Version                  Repository     Size
========================================================================
Installing:
 httpd              x86_64     2.2.15-5.el6.centos        base         811 k
 mysql              x86_64     5.1.52-1.el6_0.1           updates      889 k
 mysql-server       x86_64     5.1.52-1.el6_0.1           updates      8.1 M
 php                x86_64     5.3.2-6.el6_0.1            updates      1.1 M
 php-gd             x86_64     5.3.2-6.el6_0.1            updates      103 k
 php-mbstring       x86_64     5.3.2-6.el6_0.1            updates      504 k
 php-mysql          x86_64     5.3.2-6.el6_0.1            updates       75 k
Installing for dependencies:
 apr                x86_64     1.3.9-3.el6_0.1            updates      124 k
 apr-util           x86_64     1.3.9-3.el6_0.1            updates       87 k
 apr-util-ldap      x86_64     1.3.9-3.el6_0.1            updates       15 k
 httpd-tools        x86_64     2.2.15-5.el6.centos        base          68 k
 libXpm             x86_64     3.5.8-2.el6                base          59 k
 perl-DBD-MySQL     x86_64     4.013-3.el6                base         134 k
 php-cli            x86_64     5.3.2-6.el6_0.1            updates      2.2 M
 php-common         x86_64     5.3.2-6.el6_0.1            updates      516 k
 php-pdo            x86_64     5.3.2-6.el6_0.1            updates       72 k
Updating for dependencies:
 mysql-libs         x86_64     5.1.52-1.el6_0.1           updates      1.2 M
Transaction Summary
========================================================================
Install      16 Package(s)
Upgrade       1 Package(s)
Total download size: 16 M
```

## 28.2 配置Apache

编辑Apache配置文件，配置ServerName参数，此参数在CentOS 6.x版本以前是不需要配置的，但是CentOS 6.x之后就必须要配置，不配置就会出现警告信息，但是可以正常启动，ServerName参数若目前没有FQDN，则只要将#号删除，待往后再进行配置即可。

检查Apache支持的字符集编码，这个配置要根据软件编码是UTF-8还是GB2312来确定，Apache默认编码为UTF-8，若要安装的软件编码为GB2312，则必须修改为GB2312，不然会出现乱码问题。

配置索引首页优先级，所谓的索引首页优先级，就是说在浏览器输入【http://网址或IP地址/index.html】，如果有配置索引首页，只要输入【http:// 网址或IP地址】，就可以打开网站首页，Apache默认索引首页文件为index.html，如果创建的网站使用PHP语言页面，则首页文件

名通常为index.php，为了方便使用者，建议在index.html前面加上index.php，让index.php作为默认的索引首页。

```
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf     //编辑 Apache 配置文件
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.  See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
ServerName www.example.com:80                        //默认未配置，将#号删除
…….省略………..
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
# The index.html.var file (a type-map) is used to deliver content-
# negotiated documents.  The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
DirectoryIndex index.php index.html index.html.var
…….省略………..                  //网站默认索引首页文件，建议加上 index.php
# Specify a default charset for all content served; this enables
# interpretation of all content as UTF-8 by default.  To use the
# default browser choice (ISO-8859-1), or to allow the META tags
# in HTML content to override this choice, comment out this
# directive:
#
AddDefaultCharset UTF-8          //默认为 UTF-8，若软件编码为 GB2312，必须修改为 GB2312
```

## 28.3 启动Apache和MySQL服务

Apache服务配置完成后，接下来就可以启动Apache和MySQL服务了，PHP不是应用服务，所以无需启动。

```
[root@localhost ~]# service httpd start   //启动 Apache 服务
Starting httpd:                [  OK  ]
[root@localhost ~]# service mysqld start
                                          // Mysql 默认第一次启动会有说明，下次启动则不会再出现
Initializing MySQL database:  Installing MySQL system tables...
OK
Filling help tables...
OK
To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system
PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:
/usr/bin/mysqladmin -u root password 'new-password'
```

```
/usr/bin/mysqladmin -u root -h localhost.localdomain password 'new-password'
Alternatively you can run:
/usr/bin/mysql_secure_installation
which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
See the manual for more instructions.
You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &
You can test the MySQL daemon with mysql-test-run.pl
cd /usr/mysql-test ; perl mysql-test-run.pl
Please report any problems with the /usr/bin/mysqlbug script!
                                           [  OK  ]
Starting mysqld:                           [  OK  ]
```

Apache及MySQL服务为LAMP的必要服务，所以必须配置为开机默认启动，以免重新启动系统后忘记启动这些服务，导致无法使用。

```
[root@localhost ~]# chkconfig httpd on      //配置 Apache 默认启动
[root@localhost ~]# chkconfig mysqld on     //配置 MySQL 默认启动
```

## 28.4 配置MySQL数据库

LAMP配置软件在MySQL数据库方面，有几个操作是必要的，其操作方式如下表所示。

| 操作信息 | 命令 |
|---|---|
| 启动数据库 | service mysqld start |
| 暂停数据库 | service mysqld stop |
| 重新启动数据库 | service mysqld restart |
| 查看数据库是否运行 | service mysqld status |

下面配置MySQL数据库密码，MySQL数据库安装好后，第一次启动MySQL数据库不用输入密码，所以必须要配置密码才比较安全。配置MySQL数据库密码前，记得要先启动MySQL数据库，否则会找不到MySQL数据库。命令说明如下表所示。

| 配置密码命令说明 | Mysqladmin -u 用户 password 密码 |
|---|---|

这里配置root用户账号，密码配置为Aa1234567，配置好MySQL数据库密码后，测试是否可以正常登录，数据库配置密码后，需要在命令中添加参数[-p]，登录成功后，若要退出MySQL数据库，输入【exit】。

```
[root@localhost ~]# mysqladmin -u root password Aa1234567
                                             //配置 MySQL 用户密码
[root@localhost ~]# mysql -u root -p         //加上参数 p，以密码的方式登录
Enter password:                              //输入所配置的 MySQL 密码
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.1.52 Source distribution
Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
```

```
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> exit                                   //正常登录后，离开 MySQL 数据库
Bye

[root@localhost ~]#
```

配置完MySQL数据库密码后，在登录MySQL数据库时，若没有加上参数P，会出现Access denied警告信息。

```
[root@localhost ~]# mysql -u root
ERROR 1045 (28000) : Access denied for user 'root'@'localhost' (using password: NO)
```

使用MySQL数据库最常见的操作，不外乎是查看数据库、创建数据库、删除数据库，如果要完成更细致的操作，建议使用MySQL数据库管理软件来管理操作，例如使用phpMyAdmin或免费的Navicat for MySQL软件。

MySQL数据库的创建、删除、查看命令说明如下表所示。

| 操作 | 命令 |
|---|---|
| 创建数据库 | create database 数据库名称; |
| 查看数据库 | show databases; |
| 删除数据库 | drop database 数据库名称; |

下面创建一个名为DB1的数据库，要先登录MySQL数据库才可以配置。

```
[root@localhost ~]# mysql -u root -p    //登录 MySQL 数据库
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.1.52 Source distribution
Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> create database DB1;             //创建 DB1 数据库
Query OK, 1 row affected (0.00 sec)
mysql> show databases;                  //查看 MYSQL 内所有数据库
+--------------------+
| Database           |
+--------------------+
| information_schema |
| DB1                |                  //刚创建的 DB1 数据库
| mysql              |
| test               |
+--------------------+
4 rows in set (0.00 sec)
mysql> drop database DB1;               //删除 DB1 数据库
```

```
Query OK, 0 rows affected (0.00 sec)
```

## 配置防火墙

Apache及MySQL数据库配置启动完成后，需要在防火墙配置文件中开启Apache服务的80端口和MySQL数据库3306端口，若MySQL数据库不对外提供服务，则无需开启，在此示例中都要对外提供服务，所以防火墙必须配置Apache及MySQL数据库的端口。

```
[root@localhost ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
                                                    //开启 Apache 服务 80 端口
-A INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
                                              //开启 MySQL 数据库服务 3306 端口
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

防火墙配置完成后，必须重新启动防火墙服务，配置才会生效。

```
[root@localhost ~]# service iptables restart
iptables: Flushing firewall rules:                          [  OK  ]
iptables: Setting chains to policy ACCEPT: filter           [  OK  ]
iptables: Unloading modules:                                [  OK  ]
iptables: Applying firewall rules:                          [  OK  ]
```

再次提醒，利用LAMP软件环境创建网站前，先将上述环境配置好，需要将Apache及MySQL数据库服务启动，并将服务设为默认启动。

# 第29章

# 网站管理系统

网站管理系统就是将各种网站应用系统整合到一个信息管理平台之上，主要提供信息、搜索引擎、聊天室、论坛（BBS）、免费信箱、影音信息、电子商务、网络社区、网络游戏、免费网页空间等功能。网站管理系统在企业中较常用，目前市面上众多的网站管理软件中，使用最多的就是XOOPS，不过近几年使用Drupal的人也越来越多，下面举例介绍如何配置两种网站管理系统。

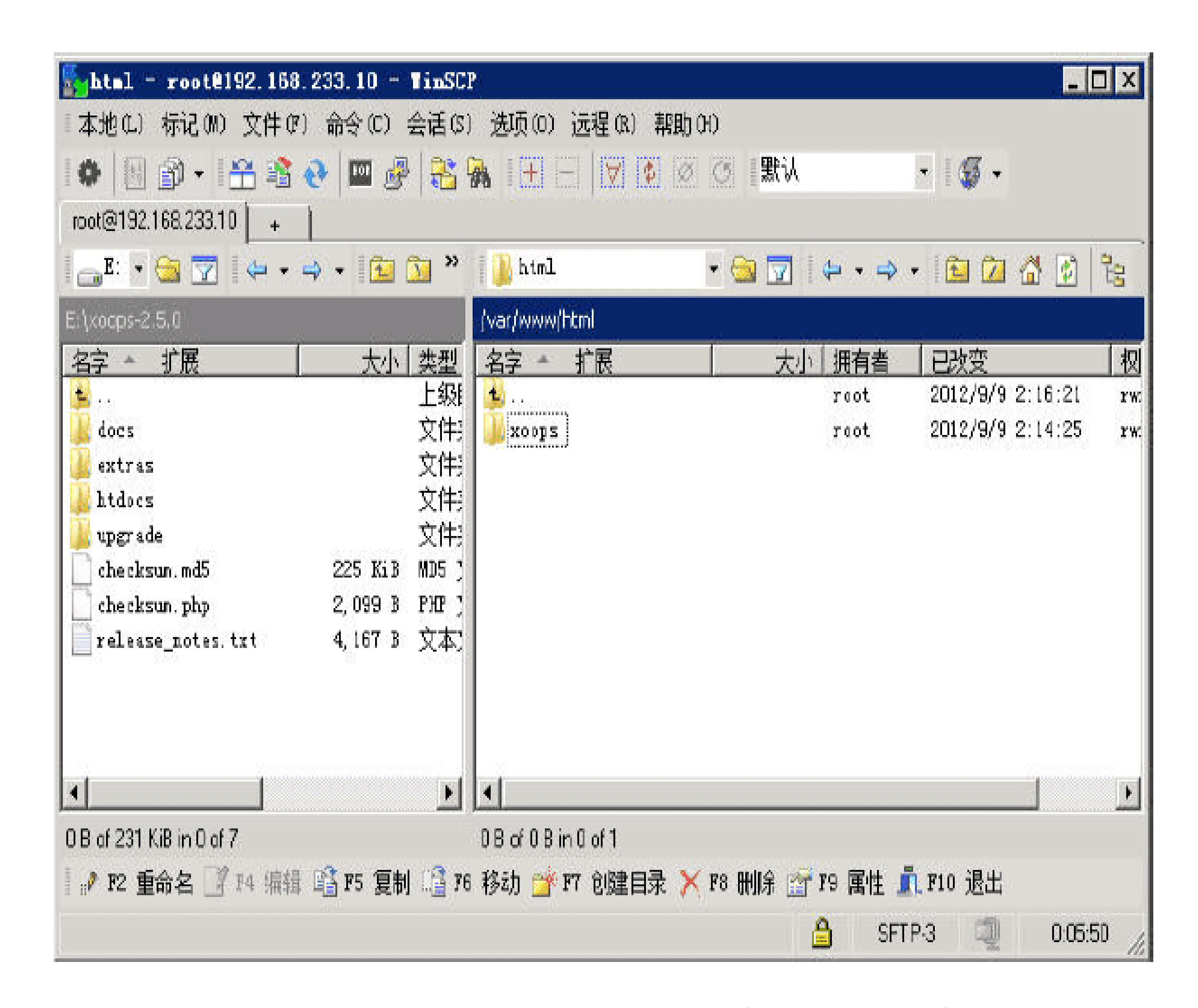
## 29.1 XOOPS内容管理系统

XOOPS官方网站：http://www.xoops.org。

XOOPS的缩写是 eXtensible Object Oriented Portal System 。XOOPS是一款开源的内容管理系统，衍生自PHP-Nuke，采用PHP语言和MySQL数据库。其功能、界面全部使用模板化设计，可用于构建各种网络站点。XOOPS的发布采用GPL协议，在遵循GPL相关条款的前提下，可免费使用和修改，可自由再发布。支持二十种以上的语言版本，包括英文、简体中文、繁体中文，编码可自由选择，可采用GB 2312、BIG 5或UTF-8。

### 安装前配置XOOPS软件

参考LAMP建站基本需求安装好LAMP环境，然后将XOOPS软件上传到LAMP服务器，利用WinSCP工具将XOOPS软件内的htdocs目录上传到Apache网页目录（/var/www/html），并将文件夹重命名为【xoops】，如下图所示。

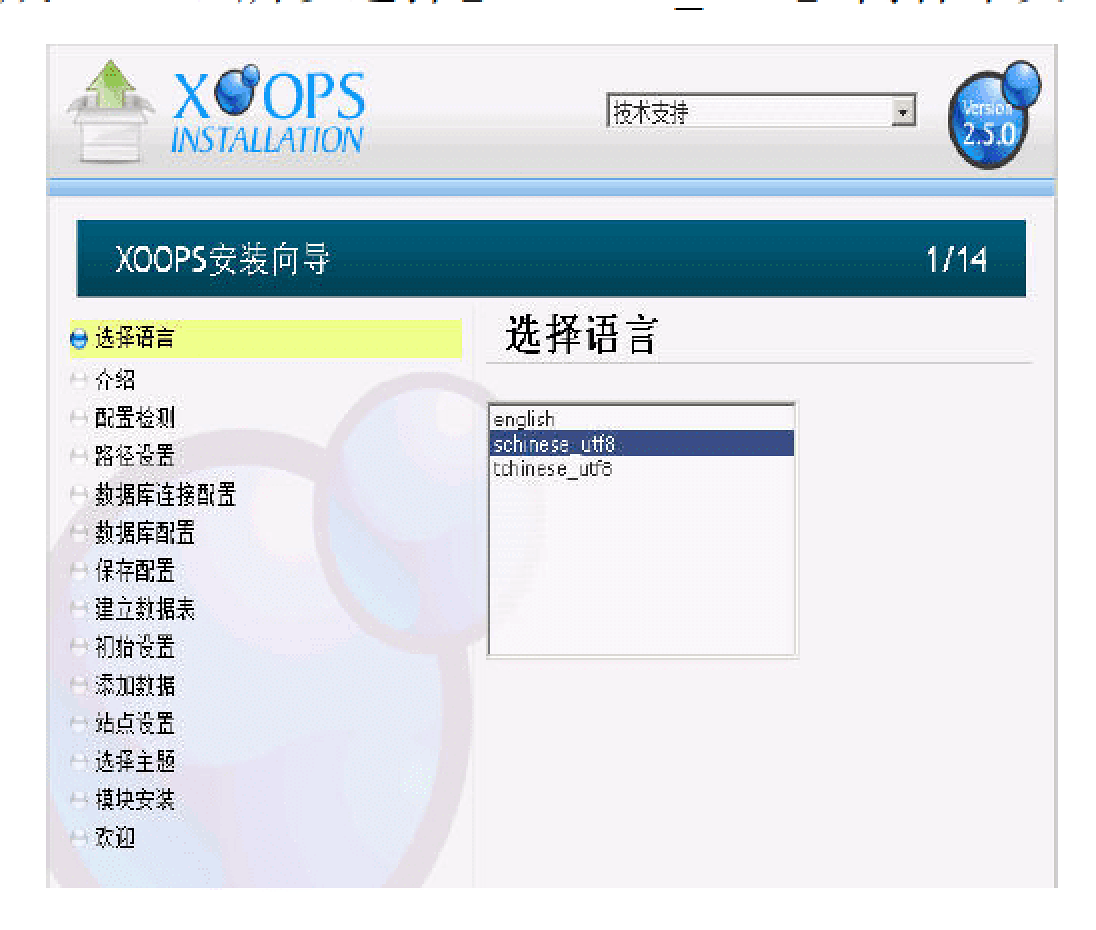


检查Apache编码是否为UTF-8，如果不是UTF-8编码，则修改成UTF-8，其实不一定要选择UTF-8，也可以选择BIG5，不过XOOPS很重视编码，所以安装XOOPS软件时选择一种编码后，就要配置该编码，以免出现问题。

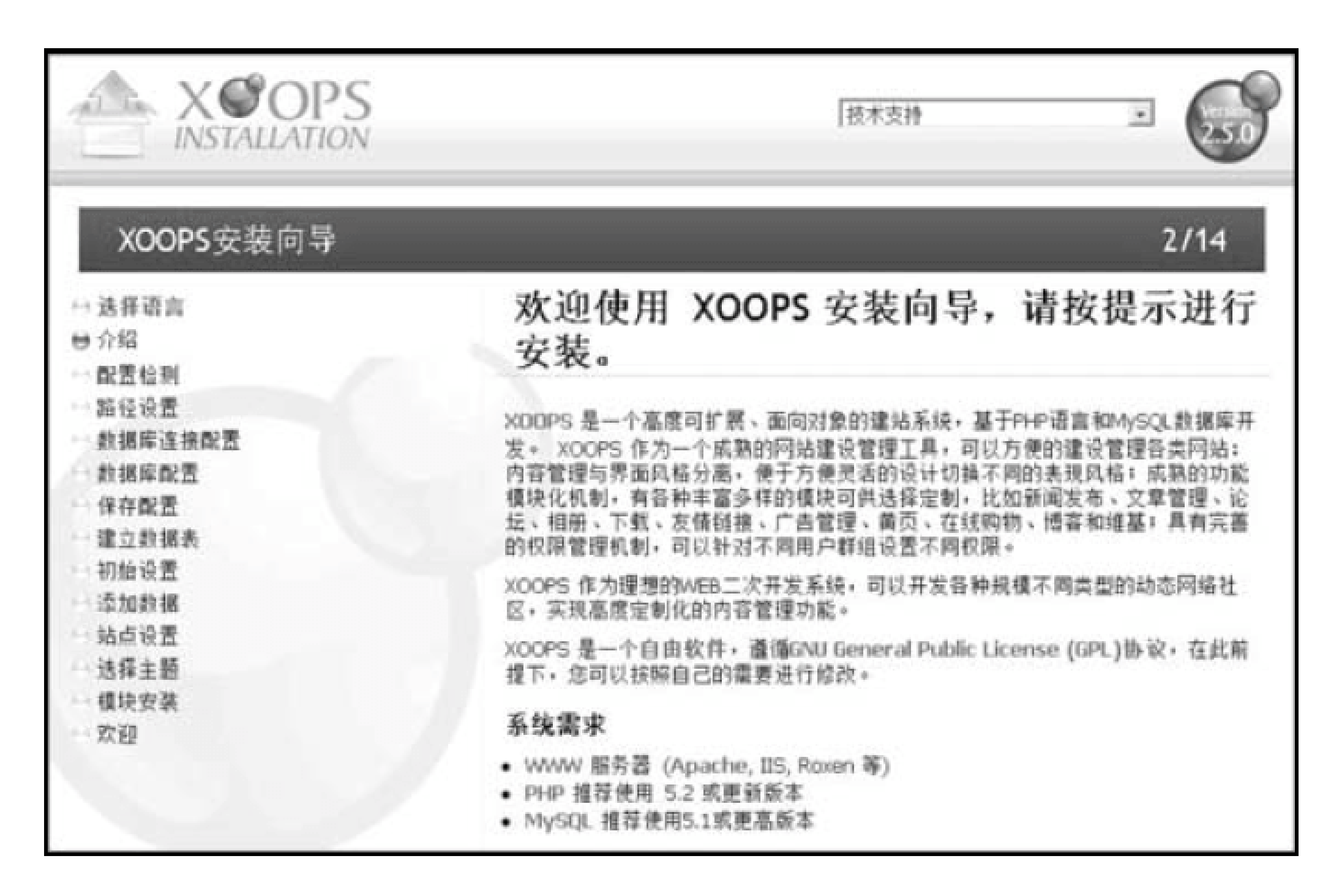
创建一个名称为【xoops】的数据库供XOOPS系统使用，若不知如何创建数据库，可以参考LAMP建站基本需求安装软件，来创建XOOPS所需要的数据库。

## 安装XOOPS软件

在浏览器中输入【http://IP地址/xoops】 开始安装XOOPS软件，在开始就必须选择编码，前面将Apache编码配置成UTF-8，所以选择【schinese_utf8】(简体中文UTF-8版)，按【下一步】。




出现XOOPS安装向导欢迎界面，显示系统需求及需修改目录的权限，需要把xoops_data和xoops_lib目录转移到网站根目录以外的目录，此步骤要在XOOPS安装完成后再进行配置。




系统环境在前面已经配置，所以只要修改目录权限即可。将下面所列出的目录或文件权限都设为777，在XOOPS安装完成后，再将mainfile.php权限修改回444。

```
uploads/
uploads/avatars/
uploads/images/
uploads/ranks/
uploads/smilies/
mainfile.php
include/license.php
xoops_data/data/secure.php
xoops_data/caches
xoops_data/caches/xoops_cache
xoops_data/caches/smarty_cache
xoops_data/caches/smarty_compile
xoops_data/configs
```

先将目录切换到XOOPS软件目录，再将上面的目录或文件权限配置为777。

```
[root@localhost /]# cd /var/www/html/xoops          //进入 XOOPS 主程序目录
[root@localhost xoops]# chmod 777 uploads uploads/avatars/ uploads/images/ uploads/ranks/
uploads/smilies/ mainfile.php include/license.php xoops_data/data/secure.php
xoops_data/caches xoops_data/caches/xoops_cache xoops_data/caches/smarty_cache
xoops_data/caches/smarty_compile xoops_data/configs      //配置所有目录及权限
```

完成所有配置后，XOOPS安装向导会自动检查基本需求是否符合。



| 基本需求 | |
|---|---|
| 服务程序接口 | apache2handler<br>Apache/2.2.15 (CentOS) |
| PHP 版本 | ✔ 5.3.3 |
| MySQL 扩展 | ✔ 5.1.61 |
| Session 扩展 | ✔ 完成 |
| PCRE 扩展 | ✔ 完成 |
| file_uploads | ✔ ON |

扩展程序需要某些功能的支持，所以尽量使所有程序都启用，避免无法使用，确认完成后，按【下一步】。



推荐启用的扩展程序

这些扩展程序不是普通用户必须安装和启用的，但是一些功能需要这些扩展的支持（例如多字节语言或RSS支持等）。因此，推荐安装和启用这些扩展程序。

| | |
|---|---|
| 字符集编码 扩展 | ✔ MBString |
| 字符集转换 扩展 | ✔ Iconv |
| XML parsing 扩展 | ✔ XML |
| Zlib 压缩 扩展 | ✔ Zlib |
| 图形函数 扩展 | ✔ GD bundled (2.0.34 compatible) |
| 图像元数据 (exif) 扩展 | ✔ Exif |

在【路径设置】选项中需要配置物理路径及虚拟路径，物理路径为LAMP服务器上的XOOPS软件目录路径，虚拟路径则是对外的URL，这是XOOPS安装向导自动默认的配置，除非有错误，否则尽量不要修改配置，以免无法安装XOOPS，按【下一步】。

路径设置

XOOPS 物理路径

XOOPS 物理路径：

/var/www/html/xoops ✔XOOPS 2.3.3 检测正确

XOOPS 数据文件

/var/www/html/xoops/xoops_data ✔路径检测正确。

XOOPS 公用类库

/var/www/html/xoops/xoops_lib ✔路径检测正确。

XOOPS 虚拟路径

XOOPS 虚拟路径(URL)：

http://192.168.233.10/xoops

上一步 下一步

下面进行数据库连接配置，因为使用的是MySQL数据库，所以数据库类型选择【mysql】，数据库主机名配置为localhost或本机IP地址，如果数据库主机是其他服务器的数据库，则输入数据库服务器的IP地址，数据库账号和密码则输入创建XOOPS数据库的账号和密码，例如创建数据库的账号是root，则输入root的账号和密码，配置完成后，按【下一步】。

数据库连接配置

数据库服务器连接配置

选择要使用的数据库类型 mysql

数据库主机名称：

localhost

数据库用户账号：

root

数据库用户密码：

•••••••

数据库持续连接：

上一步 下一步

在【数据库配置】界面中，还要配置XOOPS数据库名称，如数据库名称为xoops，其他配

置不变，配置完成后，按【下一步】。




将所有配置写入mainfile.php及secure.php文件中，写入前最好先确认，确认无误后，按【下一步】进行配置。




写入mainfile.php及secure.php后，XOOPS安装向导接下来就创建数据表，创建数据表成功后，按【下一步】。




然后创建XOOPS管理者账号数据，输入网站管理员账号、邮件账号及密码，输入密码时会识别安全级别，主要是为安全性考虑，目前很多系统都有密码复杂度设计，如果自己无法想出较复杂的密码，也可以使用系统帮你生成密码，配置输入完成后，按【下一步】。

请输入初始设置

管理员账号设置
网站管理员帐号：
jerry
网站管理员邮件：
jerry@jerryit.idv.cn
网站管理员密码：
•••••••
确认管理员密码：
•••••••
密码强度：
一般
密码生成器
生成 复制
上一步 下一步

关于密码复杂度可以参考如下内容。

- 密码长度至少为 6 个字符。
- 至少包含下列 4 种字符类型中的 3 种：小写英文字母（a ~ z）、大写英文字母（A ~ Z）、数字（0 ~ 9）、特殊字符（如!、$、#、% 等）。
- 不能包含用户账号的某一部分字符（超过 2 个字符）。

站点设置分为几部分，即基本参数设置、Meta及页脚、会员管理设置；基本参数设置主要是设置网站名称及网站口号，XOOPS安装向导会自动使用默认值，可以依需求修改。

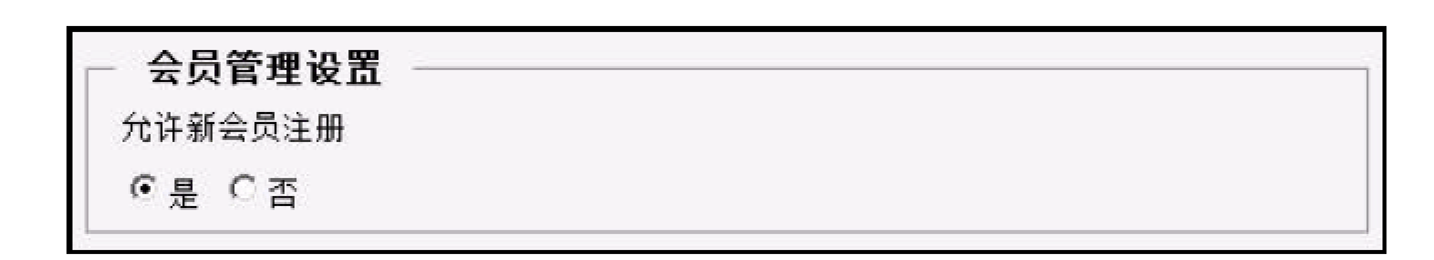
站点设置

基本参数设置
网站名称
XOOPS Site
网站口号
Just Use it!

依需求配置Meta关键字、描述、作者、版权数据。

Meta 及页脚
Meta 关键字
xoops, web applications, web 2.0, sns, news, technology, headlines, linux, software, download, downloads, free, community, forum, bulletin board, bbs, php, survey, polls, kernel, comment, comments, portal, odp, open source, opensource, FreeSoftware, gnu, gpl,
Meta 描述
XOOPS is a dynamic Object Oriented based open source portal script written in PHP.
META作者
XOOPS
Meta 版权
Copyright © 2001-2012

会员管理设置用于配置是否允许新会员注册，默认为否，这里配置为【是】，此配置也可以在管理后台开启，按【下一步】。




选择网站默认风格，此版本默认有三种风格可供选择，选择完毕后，按【下一步】。




模块安装，此版本默认提供了三种可以安装的模块，即站内短信、用户管理、protector（防护模块），将所有配置选为【是】进行安装，也可以在安装完后，根据需求安装其他模块，增加Xoops功能性，按【下一步】。

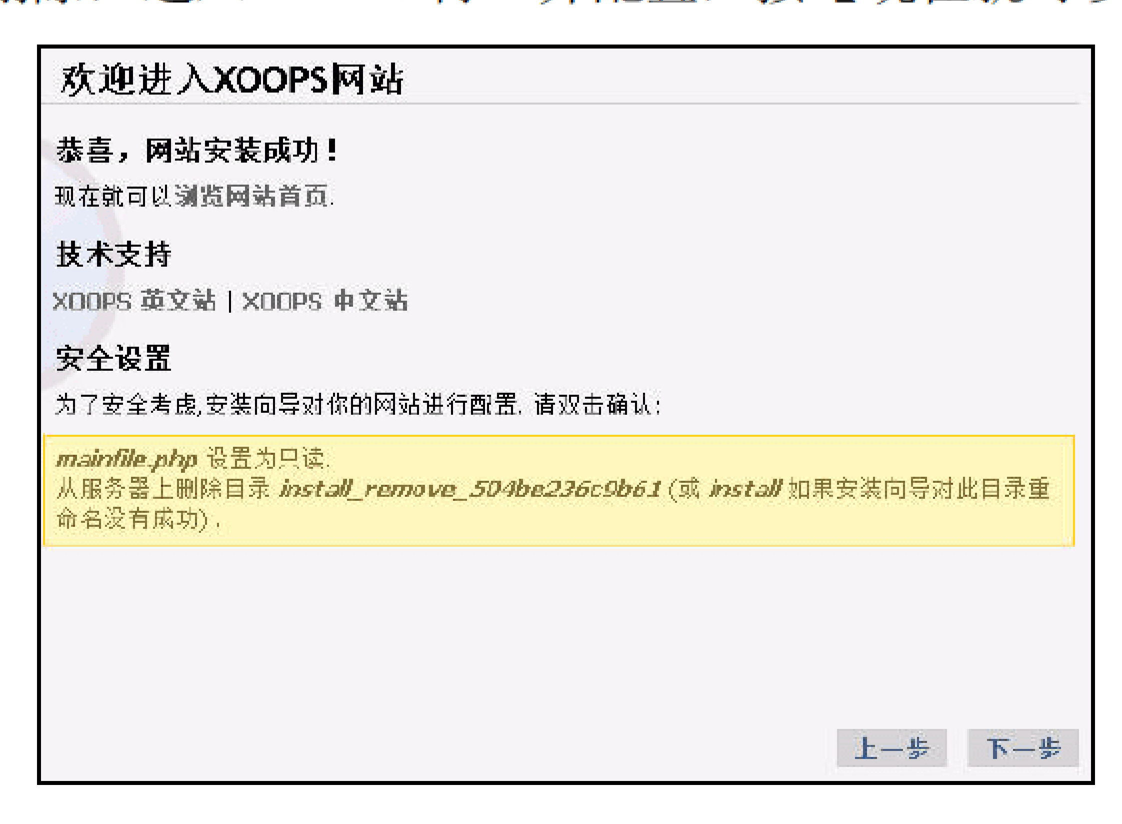



XOOPS模块安装完成后，按【下一步】。

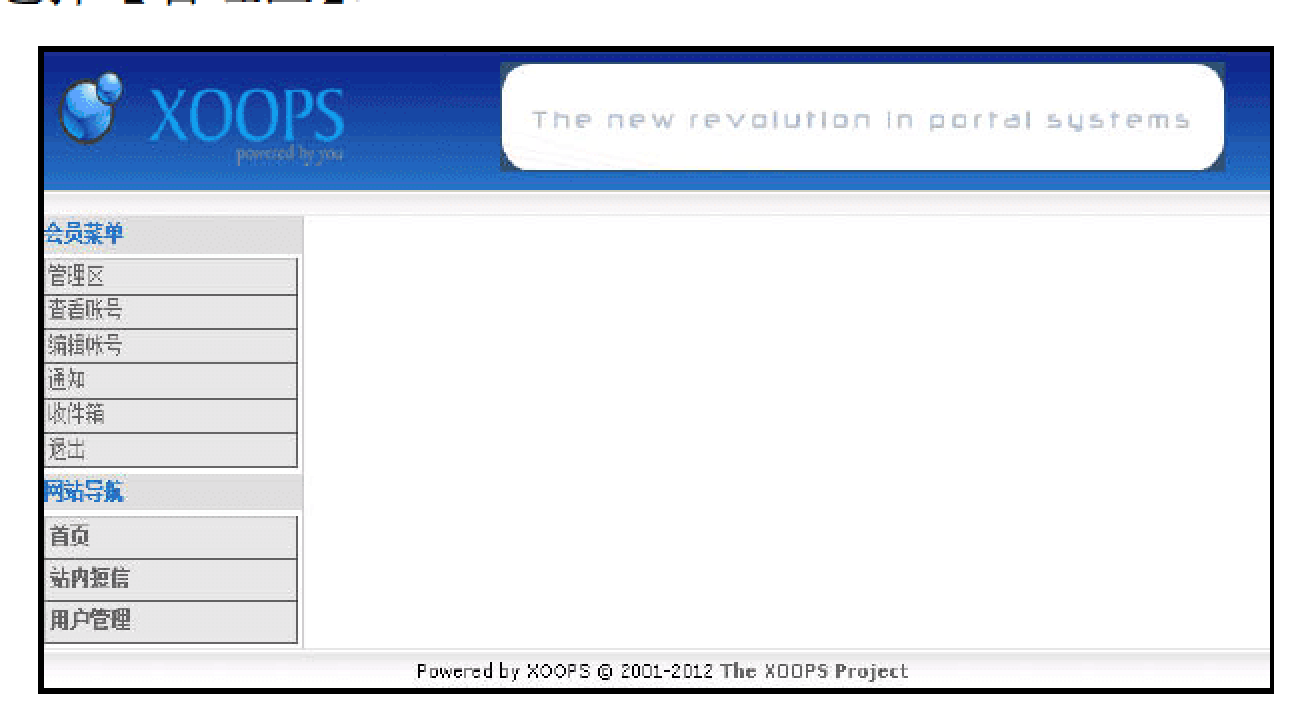



至此XOOPS软件安装完成，接下来进入刚创建的网站！在进入XOOPS网站前，基于安全

考虑，将一开始安装的mainfile.php权限配置为写入，不过先不要修改mainfile.php权限，也不要将install目录改名或删除，进入XOOPS再一并配置，按【现在就可以浏览网站首页】。




XOOPS网站路径为【http://IP地址/xoops】，XOOPS安装完后，按【现在就可以浏览网站首页】直接进入网站，所以管理者账号即为已登录状态，不过下次登录时就必须输入管理员账号和密码，先单击选择【管理区】。




管理区内会出现4个警告，不修改也可以使用，但是为了安全性考虑还是做一下修改。

第一个警告提示需将XOOPS主程序的install安装目录删除或重命名。

第二个警告提示要将mainfile.php权限属性配置为444。

第三个和第四个警告则提示需将xoops_lib（公共类库）及xoops_data（XOOPS数据）目录转移到网站根目录以外的路径，Apache网页默认目录为/var/www/html，网站目录以外的路径就是指非该路径即可。



先将install安装目录改名为install_old，再将xoops_lib（公共类库）及xoops_data（XOOPS数据）目录转移至/var/www目录下，然后修改mainfile.php文件，将这两个目录路径修改，修改完毕后，再将mainfile.php权限配置为444。

```
[root@localhost ~]# cd /var/www/html/xoops                 //进入 XOOPS 目录
[root@localhost xoops]# mv install install_old        //重命名 XOOPS 安装目录
[root@localhost xoops]# mv xoops_data  xoops_lib  /var/www
                              //将 xoops_data 和 xoops_lib 目录转移到/var/www
[root@localhost xoops]# vi mainfile.php
                                      //修改 xoops_data 和 xoops_lib 目录路径
  // For forward compatibility
  // Physical path to the XOOPS library directory WITHOUT trailing slash
  define（'XOOPS_PATH', '/var/www/xoops_lib'）;  //xoops_lib 转移后路径
  // Physical path to the XOOPS datafiles（writable）directory WITHOUT
  trailing slash
  define（'XOOPS_VAR_PATH', '/var/www/xoops_data'）;
                                                   //xoops_data 转移后路径
  // Alias of XOOPS_PATH, for compatibility, temporary solution
  define（"XOOPS_TRUST_PATH", XOOPS_PATH）;
[root@localhost xoops]# chmod 444 mainfile.php  //修改 mainfile.php 权限属性
```

重新单击管理后台页面，所有警告消息都消失，这时就可以开始使用XOOPS系统了。




## 29.2 Drupal（水滴）内容管理系统

Drupal英文官方网站：http://drupal.org/。

Drupal 简体中文网站：http://drupalchina.cn/。

Drupal 官方模块下载地址：http://drupal.org/project/Modules。

Drupal 简体中文网站模块下载地址：http://drupalchina.cn/download。

Drupal模板下载地址：http://drupal.org/project/themes。

Drupal致力于通过为其用户提供所需的工具来建立其自己的内容管理解决方案的方式来

实现各项管理功能，同时还提供一些预建的组件来帮助用户入门。已经有许多个人和组织采用Drupal来创建各种不同的网站，包括：

- 社区论坛和讨论区
- 企业网站/企业内部入口网站
- 个人网站或blog
- 专题网站
- 电子商务应用
- 资源分类目录
- 社交网站

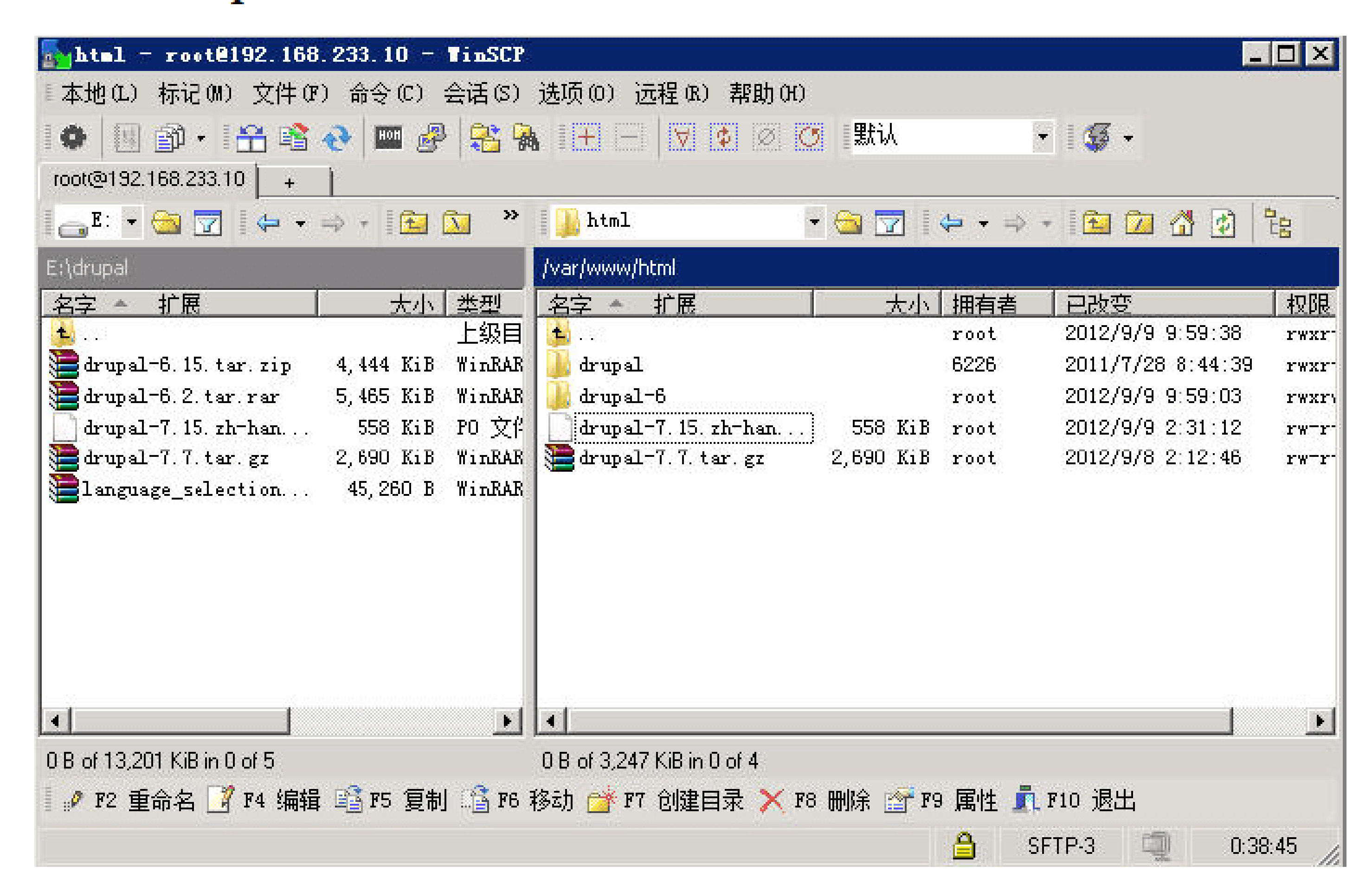
Drupal包括以下功能：

- 内容管理系统
- blog
- 共同写作环境
- 讨论区
- 同侪运算网络
- 电子报
- 相册
- 文件上传与下载

Drupal是一套采用GPL授权的开放源码软件，是由数以千计的使用者和开发人员所共同维护和开发的。如果你喜欢Drupal，请与我们一起努力，扩充并改善Drupal，使它更符合你的需求。

## 安装Drupal软件前的配置

参考LAMP建站软件的基本需求将环境安装好，然后将Drupal安装主程序上传到LAMP服务器上，利用WinSCP工具将Drupal压缩文件和简体中文语言文件上传到/var/www/html下，如下图所示。



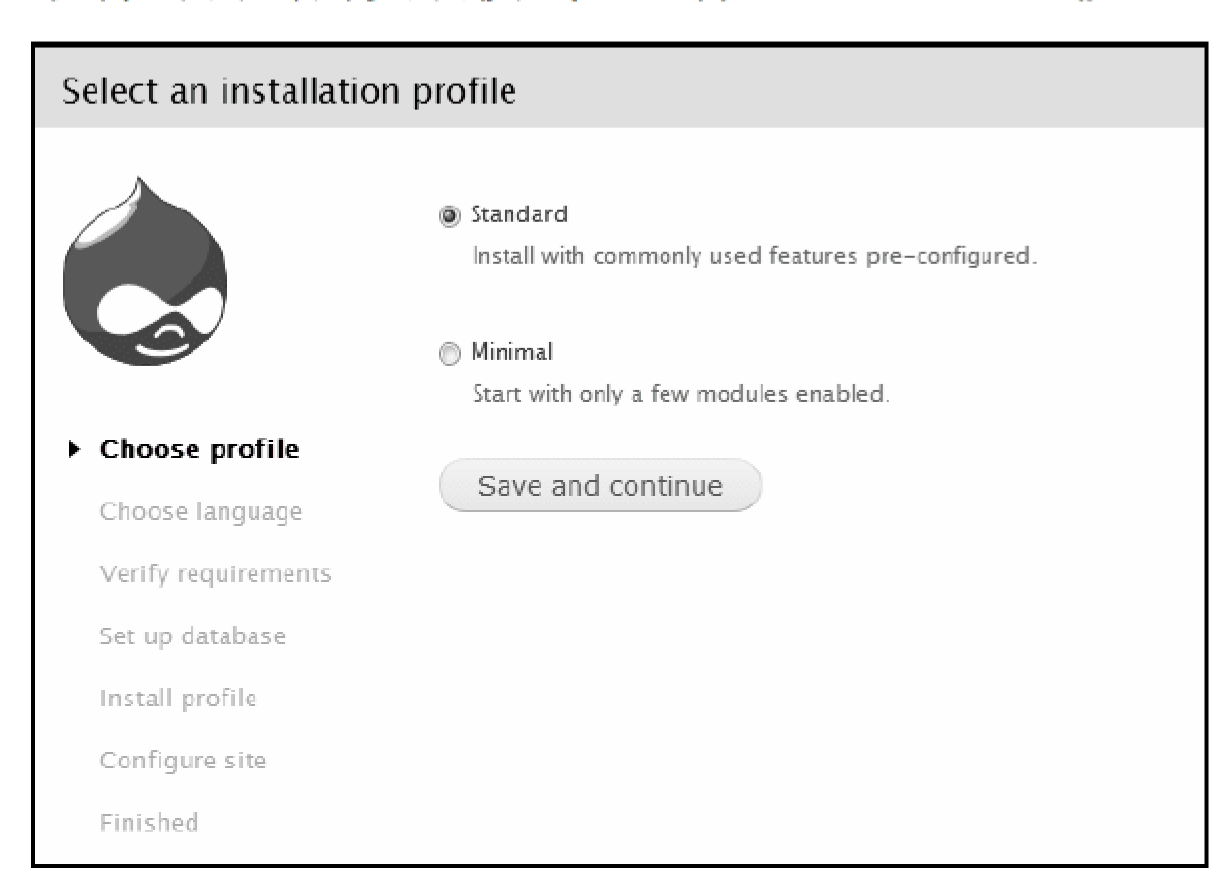
进入Apache默认网页目录，将Drupal压缩文件解压缩，并将简体中文语言文件移动至Drupal的translations目录下。

```
[root@localhost ~]# cd /var/www/html            //进入 Apache 默认网页目录
[root@localhost html]# ll                       //列出上传到网页目录的文件
total 3160
-rw-r--r--. 1 root root 2754113 Aug 15 02:26 drupal-7.7.tar.gz
-rw-r--r--. 1 root root  475765 Aug 15 23:08 drupal-7.15.zh-hans.po
[root@localhost html]# tar -zxvf drupal-7.7.tar.gz //解压缩 Drupal 压缩文件
[root@localhost html]# ll                       //列出解压缩后的 Drupal-7.7
total 3164
drwxr-xr-x. 9 6226 6226    4096 Jul 28 08:44 drupal-7.7
-rw-r--r--. 1 root root 2754113 Aug 15 02:26 drupal-7.7.tar.gz
-rw-r--r--. 1 root root  475765 Aug 15 23:08 drupal-7.15.zh-hans.po
[root@localhost html]# mv drupal-7.7  drupal          //将目录名称改为 dupal
[root@localhost html]# mv drupal-7.15.zh-hans.po drupal/profiles/standard/translations
//移动至语言文件目录
```

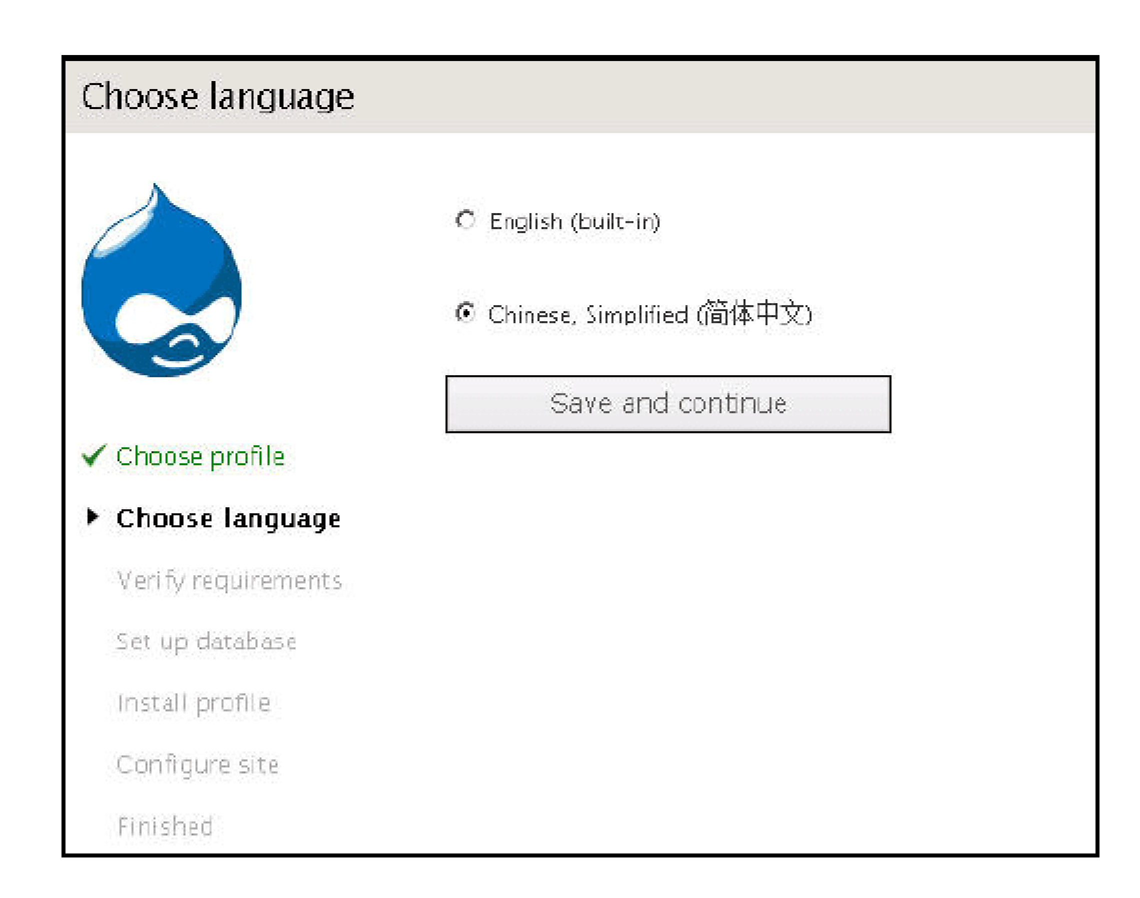
创建一个数据库让Drupal系统使用，例如数据库名称为【drupal】，若不知道如何创建数据库，可以参考LAMP软件安装需求，创建Drupal软件所需要的数据库。

## 安装Drupal软件

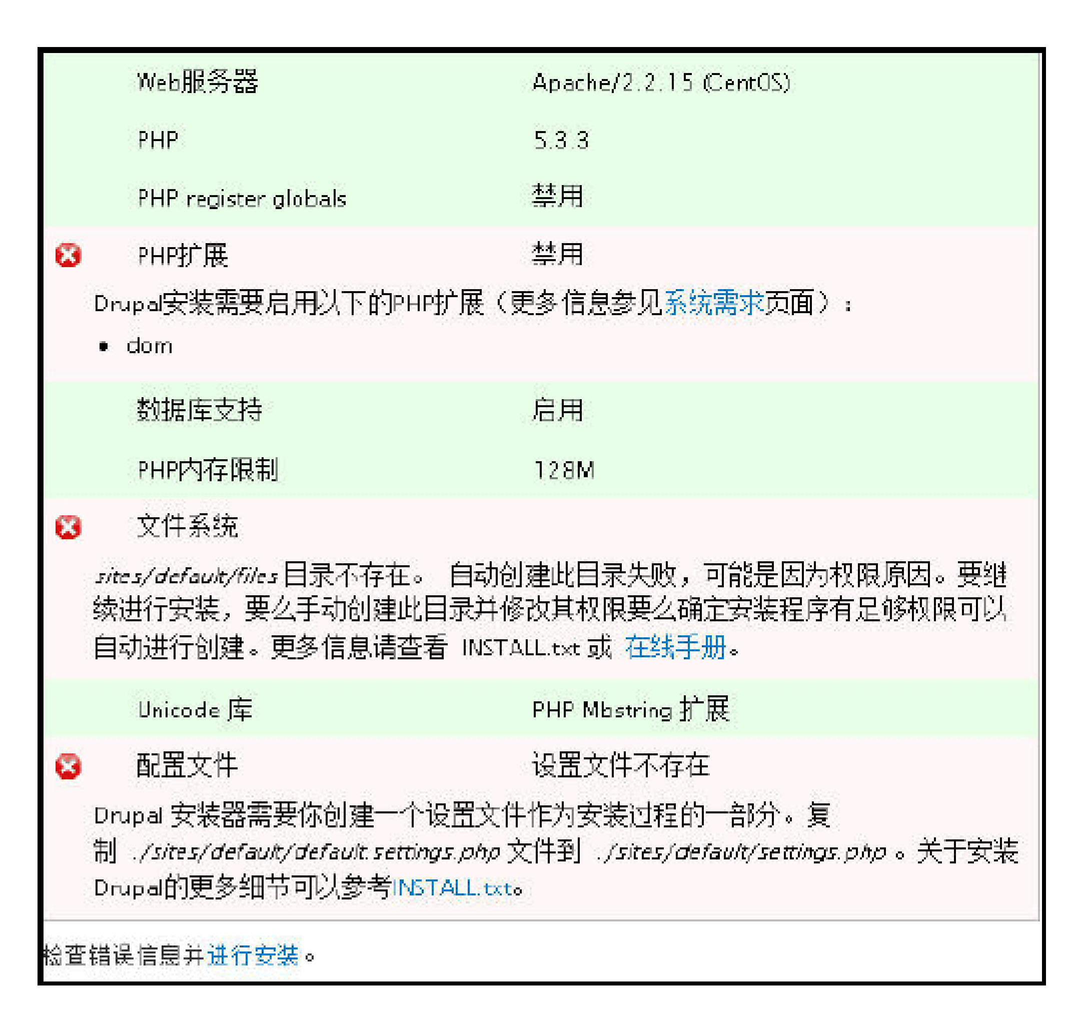
开始安装Drupal 7软件时会询问安装模式，选择【Standard】，按【Save and continue】。



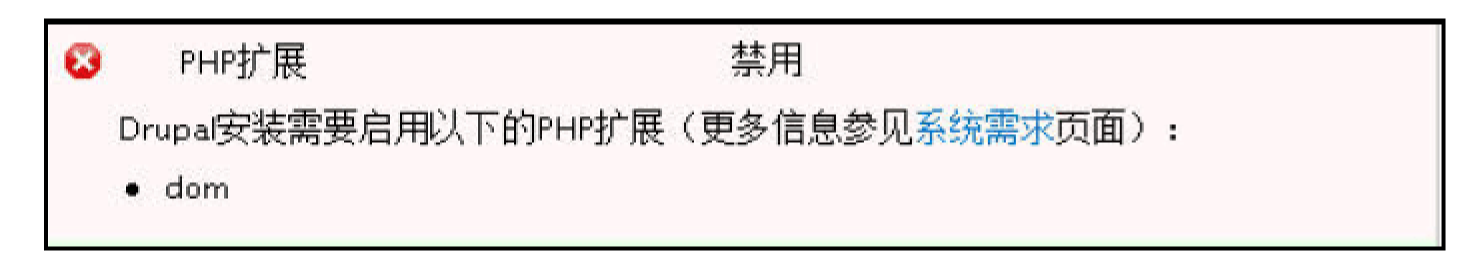

选择Drupal系统语言。软件默认只有English，因为事先将简体中文语言文件放置于/profiles/standard/translations/目录，所以会多出简体中文选项，单击选择【Chinese，Simplified（简体中文）】，按【Save and continue】。




检测系统需求时出现下列错误，如果按照LAMP建站软件需求将环境安装好，则只会出现三个错误，分别是PHP extensions已禁用、sites/default/files目录不存在、配置文件settings.php不存在。




需要修改上面因配置出现的错误信息，因为下面的任何配置都会在/var/www/html/drupal目录下执行，所以输入【cd /var/www/html/drupal】，进入该目录。使用在线更新的方法安装php-xml软件，就可以开启php扩展模块了。




```
 [root@localhost drupal]# yum install -y php-xml        //安装 php-xml 软件
Dependencies Resolved
========================================================================
 Package       Arch              Version    Repository  Size
========================================================================
Installing:
 php-xml     x86_64    5.3.2-6.el6_0.1    updates    100 k
Installing for dependencies:
```

```
 libxslt      x86_64    1.1.26-2.el6       base       450 k
Transaction Summary
=====================================================================
Install        2 Package(s)
Upgrade        0 Package(s)
Total download size: 550 k
[root@localhost drupal]# service httpd restart   //重新启动 Apache
Stopping httpd:                       [  OK  ]
Starting httpd:                       [  OK  ]
```

要修改sites/default/files目录默认不存在的错误信息，必须要创建并配置权限为777。

> 文件系统
>
> *sites/default/files* 目录不存在。 自动创建此目录失败，可能是因为权限原因。要继续进行安装，要么手动创建此目录并修改其权限要么确定安装程序有足够权限可以自动进行创建。更多信息请查看 INSTALL.txt 或 在线手册。

```
[root@localhost drupal]# mkdir sites/default/files        //创建 files 目录
[root@localhost drupal]# chmod 777 sites/default/files
                                                //配置 files 目录权限为 777
```

因为Drupal的配置文件settings.php默认不存在，必须要把sites/default目录下的default.settings.php文件复制一份并重命名为settings.php，再将权限修改为777即可。

> 配置文件　　设置文件不存在
>
> Drupal 安装器需要你创建一个设置文件作为安装过程的一部分。复制 *./sites/default/default.settings.php* 文件到 *./sites/default/settings.php* 。关于安装Drupal的更多细节可以参考INSTALL.txt。

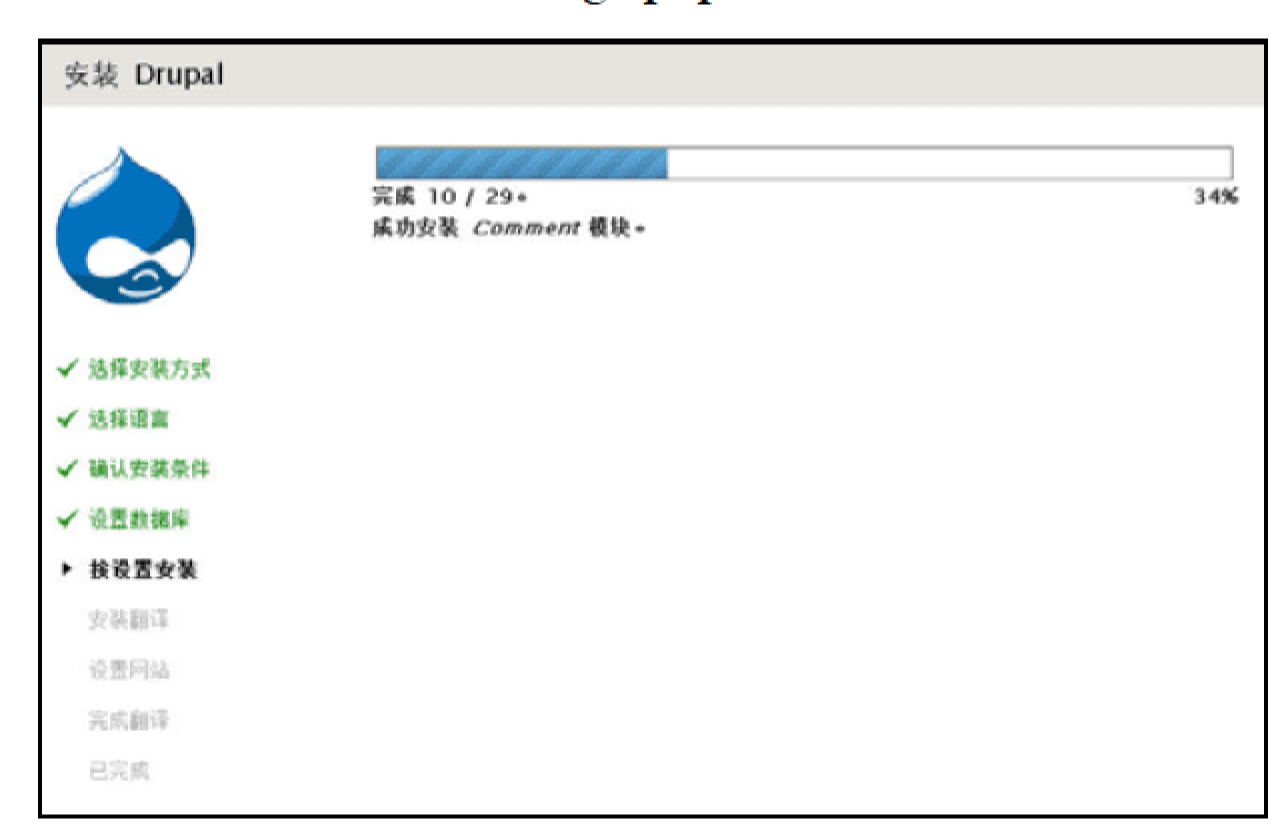
```
[root@localhost drupal]# cp sites/default/default.settings.php
sites/default/settings.php                  //复制配置文件
[root@localhost drupal]# chmod 777 sites/default/settings.php
                                      //配置可以写入权限
```

排除上述三个错误后，重新整理Drupal安装页面，则会自动进入下一个页面。

配置Drupal所要使用的数据库，数据库类型选择【MySQL，ariaDB，或者类似的】，输入数据库名称、用户名、密码，按【保存并继续】。



Drupal安装向导会将相关数据写入settings.php配置文件中。




相关数据写入settings.php配置文件后，安装向导会出现settings.php配置文件要求改成只读的提示，不过此操作可以在完成后再进行配置。



所有对于 *sites/default* 和 *sites/default/settings.php* 的必要更改已经完成，现在应当移除其可写权限以避免安全隐患。若不确定该如何操作，可以参阅在线手册。

【站点信息】选项中需要配置站点名称及网站电子邮箱。

站点信息

站点名称 *

192.168.233.10

网站电子邮箱 *

jerry@jerryit.idv.cn

自动生成的电子邮件（如注册信息）将从此地址发送。使用您的站点域名作为邮件服务器有助于避免这些邮件被视作垃圾邮件。

【站点维护账号】选项中需要配置用户名、密码，电子邮件地址会自动使用网站电子邮件地址，可以自行修改其他电子邮件地址，系统会判断密码强度，并建议合适的密码复杂度。

站点维护帐号

用户名 *

jerry

允许空格，不允许\\\".\\\"、“-”、“_”以外的其他符号。

电子邮件地址 *

jerry@jerryit.idv.cn

密码 *

●●●●●●● 密码强度： 强

确认密码 *

●●●●●●● 密码匹配： 是

增强你的密码：

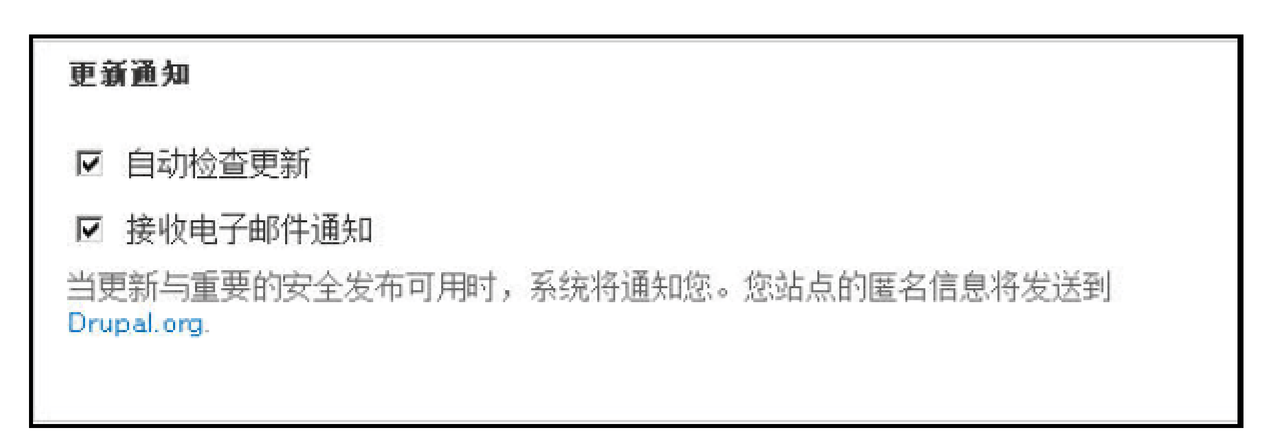
- 添加大写字母

【服务器设置】选项基本上不做任何修改，默认国家为空白，可以自行配置为中国，默认

时区会依地区而变动。




【更新通知】选项默认会选择自动检查更新和接收电子邮件通知，可依个人配置。配置完成后，按【保存并继续】。




Drupal选项安装完成，单击【访问新网站】，可以立即浏览个人Drupal网站。




或者输入【http://IP地址 /drupal/】，可以马上看到Drupal首页。




登录管理员账号后，选择【配置】→【状态报告】，可以查看目前配置状态，此处会显示上传进度和配置文件的需求配置。




若要启用上传进度，必须要安装PECL上传进度库或APC，官方建议安装PECL，所以选择安装PECL软件，安装PECL软件前除了需安装php-devel、php-pecl、php-pear软件外，还要安装Development Tools，再安装PECL uploadprogress，最后配置php.ini，所有配置完成后，重新启动Apache服务。

| 上传进度 | 未启用 |
|---|---|
| 你的服务器尚需必要的库以显示文件上传进度。推荐安装PECL上传进度库（首选）或安装APC。 | |

```
[root@localhost drupal]# yum -y install php-devel php-pecl php-pear
//安装相关 PHP 软件
Dependencies Resolved
=========================================================================
 Package          Arch        Version               Repository      Size
=========================================================================
Installing:
 php-devel        x86_64      5.3.2-6.el6_0.1       updates         502 k
 php-pear         noarch      1:1.9.0-2.el6         base            391 k
Installing for dependencies:
 autoconf         noarch      2.63-5.1.el6          base            781 k
 automake         noarch      1.11.1-1.2.el6        base            550 k
Transaction Summary
=========================================================================
Install        4  Package(s)
Upgrade        0  Package(s)
Total download size: 2.2 M
 [root@localhost drupal]# yum -y groupinstall "Development Tools"  //安装 Development Tools
Dependencies Resolved
=========================================================================
 Package          Arch     Version           Repository    Size
=========================================================================
Installing:
 Bison         x86_64      2.4.1-5.el6           base     637 k
 Byacc         x86_64      1.9.20070509-6.1.el6  base     48 k
 Cscope        x86_64      15.6-6.el6            base     136 k
 Ctags         x86_64      5.8-2.el6             base     147 k
 Diffstat      x86_64      1.51-2.el6            base     29 k
 Doxygen       x86_64      1:1.6.1-4.el6         base     2.4 M
 Flex          x86_64      2.5.35-8.el6          base     286 k
 Gcc           x86_64      4.4.4-13.el6          base     10 M
 gcc-c++       x86_64      4.4.4-13.el6          base     4.7 M
```

```
 gcc-gfortran x86_64     4.4.4-13.el6        base     4.7 M
 git          x86_64     1.7.1-2.el6_0.1     updates  4.6 M
 indent       x86_64     2.2.10-5.1.el6      base     115 k
 intltool     noarch     0.41.0-1.1.el6      base     58 k
 libtool      x86_64     2.2.6-15.5.el6      base     564 k
 patchutils   x86_64     0.3.1-3.1.el6       base     95 k
 rcs          x86_64     5.7-37.el6          base     173 k
 redhat-rpm-config noarch9.0.3-25.el6        base     56 k
 rpm-build    x86_64     4.8.0-12.el6        base     122 k
 subversion   x86_64     1.6.11-2.el6_0.3    updates  2.3 M
 swig         x86_64     1.3.40-5.el6        base     1.1 M
 systemtap    x86_64     1.2-9.el6           base     2.4 M
Updating:
 Cvs          x86_64     1.11.23-11.el6_0.1  updates  713 k
Installing for dependencies:
 cloog-ppl    x86_64     0.15.7-1.2.el6      base     93 k
 cpp          x86_64     4.4.4-13.el6        base     3.7 M
 gettext-devel x86_64    0.17-16.el6         base     155 k
 gettext-libs x86_64     0.17-16.el6         base     112 k
 glibc-devel  x86_64     2.12-1.7.el6_0.5    updates  961 k
 glibc-headers x86_64    2.12-1.7.el6_0.5    updates  592 k
 kernel-devel x86_64     2.6.32-71.29.1.el6  updates  6.5 M
 kernel-headers x86_64   2.6.32-71.29.1.el6  updates  991 k
 libart_lgpl  x86_64     2.3.20-5.1.el6      base     65 k
 libgcj       x86_64     4.4.4-13.el6        base     19 M
 libproxy     x86_64     0.3.0-2.el6         base     39 k
 libproxy-bin x86_64     0.3.0-2.el6         base     8.1 k
 libproxy-python x86_64  0.3.0-2.el6         base     8.2 k
 libstdc++-devel x86_64  4.4.4-13.el6        base     1.5 M
 mpfr         x86_64     2.4.1-6.el6         base     157 k
 neon         x86_64     0.29.3-1.2.el6      base     119 k
 pakchois     x86_64     0.4-3.2.el6         base     21 k
 perl-Error   noarch     1:0.17015-4.el6     base     29 k
 perl-Git     noarch     1.7.1-2.el6_0.1     updates  28 k
 ppl          x86_64     0.10.2-11.el6       base     1.3 M
Updating for dependencies:
 Glibc        x86_64     2.12-1.7.el6_0.5    updates  3.7 M
 glibc-common x86_64     2.12-1.7.el6_0.5    updates  14 M
Transaction Summary
========================================================================
Install      41 Package(s)
Upgrade       3 Package(s)
Total download size: 88 M
 [root@localhost drupal]# pecl install uploadprogress  //安装 PECL uploadprogress
......中间省略........
[root@localhost drupal]# vi /etc/php.ini       //编辑 php.ini
...中间省略...
extension=uploadprogress.so           //在最后一行添加的信息
[root@localhost drupal]# service httpd restart    //重新启动 Apache
Stopping httpd:                            [  OK  ]
Starting httpd:                         [  OK  ]
```

Drupal配置文件配置完成后，必须将settings.php设为只读（不可以写入），除配置文件外，

sites/default目录也必须取消写入权限。

| | |
|---|---|
| 配置文件 | 未保护 |

文件 *sites/default/settings.php* 未设置修改保护而造成安全隐患。您必须改变文件为只读。

```
[root@localhost drupal]# chmod 444 sites/default/settings.php//配置文件只读
[root@localhost drupal]# chmod 555 sites/default            //设为不可写入
```

再次重新整理页面后，所有的错误或警告都会消失，这样就可以开始使用Drupal了。

| | |
|---|---|
| Web服务器 | Apache/2.2.15 (CentOS) |
| 上传进度 | 启用（PECL 上传进度） |
| 存取 update.php | 被保护 |
| 数据库更新 | 最新的 |
| 数据库系统 | MySQL, MariaDB, or equivalent |
| 数据库系统版本 | 5.1.61 |
| 文件系统 | 可写(公开下载模式) |
| 更新通知 | 启用 |
| 节点访问权限 | 禁用 |

如果站点在内容权限上发生问题，可能需要重建权限缓存。重建缓存会清除内容的所有权限并基于当前模块及设置替换权限。如果内容量巨大或权限设置很复杂，重建缓存可能会花上一段时间。在重建缓存完成后，内容会自动使用新的权限。 重建权限

| | |
|---|---|
| 配置文件 | 被保护 |

# 第30章

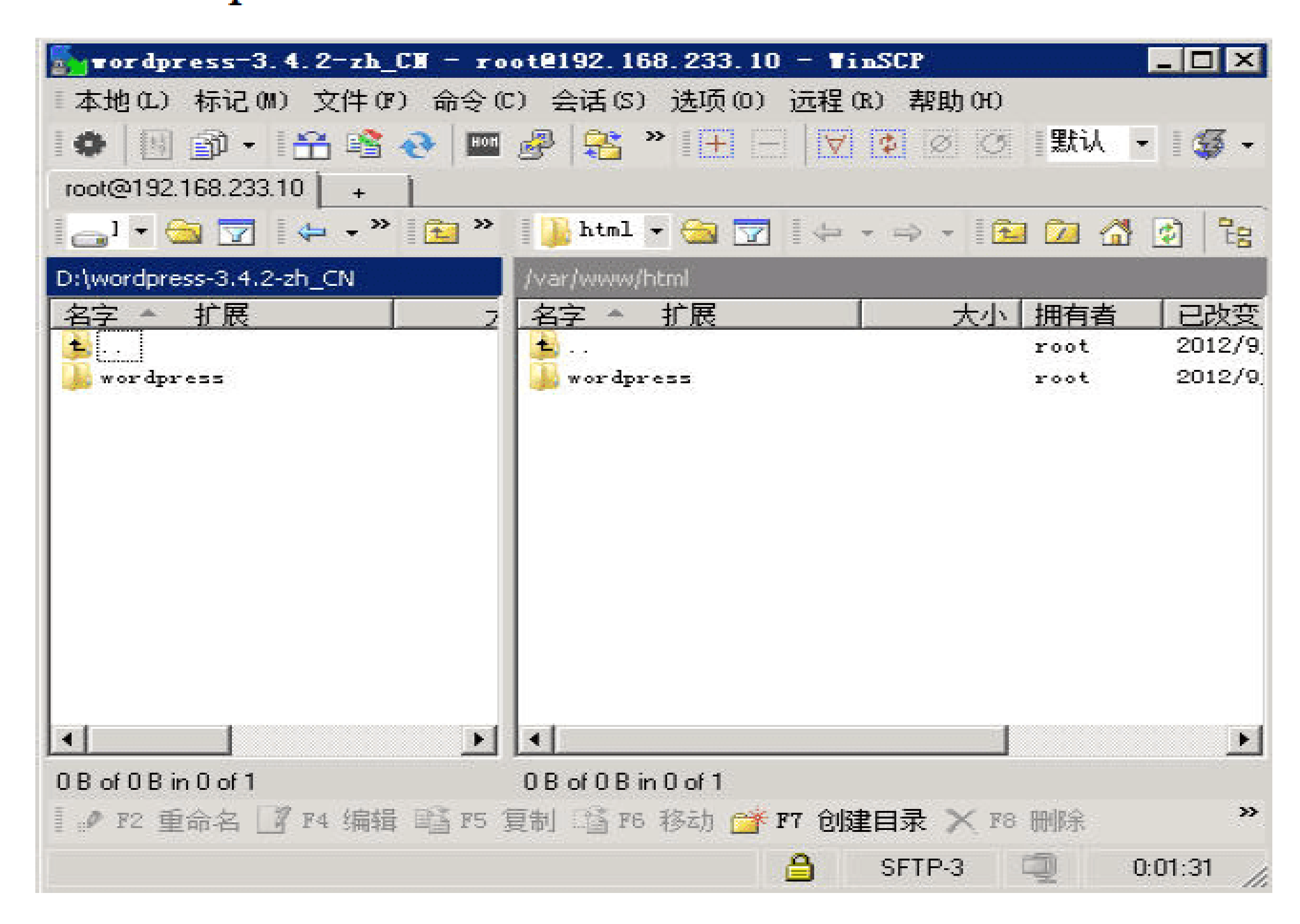
# Blog（博客）——WordPress

WordPress简体中文网站：http://cn.wordpress.org/。

WordPress是一个开放源代码的博客平台，全世界有数以百计的人正在为它付出努力。WordPress简体中文网站主要专注于 WordPress 的推广与相关信息的建立，主要提供可靠的官方WordPress中文版本、简体中文手册与相关支持，也服务于多数的商业平台。这意味着你可以完全免费地使用它，不需要支付一毛钱。WordPress成为个人创建博客的首选。

## 30.1 WordPress软件安装前的配置

参考LAMP建站软件需求将LAMP环境安装好，然后将WordPress软件上传到LAMP服务器，可以利用WinSCP工具将WordPress软件目录复制到Apache网页目录（/var/www/html）下，并将文件夹重命名为【wordpress】。




首先检查Apache配置文件是否支持UTF-8编码，如果不支持，则修改成支持UTF-8，以免浏览网页时出现乱码。在安装wordpress软件前需要建立一个名称为【wordpress】的数据库，供WordPress使用，如果不知道如何建立数据库，可以参考LAMP建站软件需求安装中的mysql

操作，来创建WordPress需要的数据库。

## 30.2 安装WordPress软件

首先进入WordPress目录，复制模板配置文件并将其重命名为wp-config.php，否则无法配置WordPress软件。

```
[root@localhost ~]# cd /var/www/html/wordpress      //进入 WordPress 目录
[root@localhost wordpress]# cp wp-config-sample.php wp-config.php
                            //复制 WordPress 模板配置文件并重命名为 wp-config.php
```

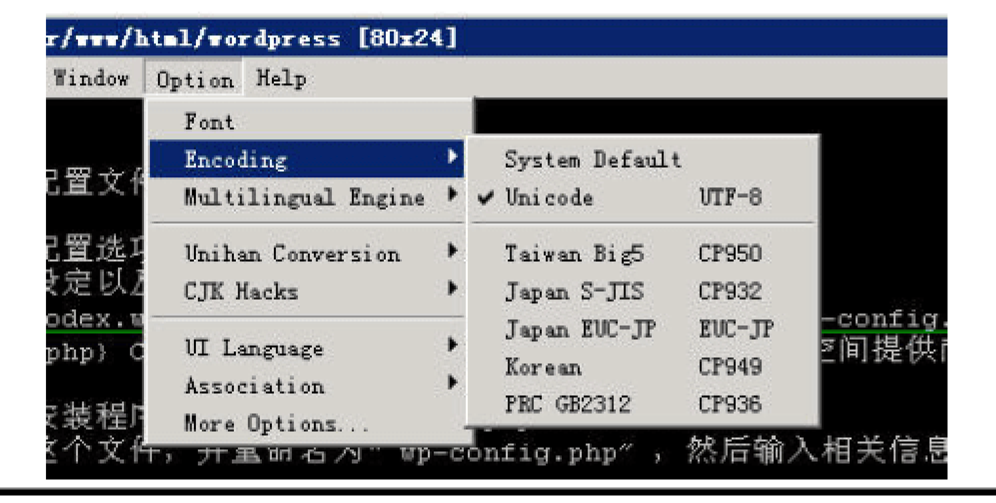
编辑WordPress配置文件，设置连接MySQL数据库的相关配置，并设置支持语言，配置完成后，保存退出。

```
[root@localhost wordpress]# vi wp-config.php        //编辑 WordPress 配置文件
// ** MySQL 配置 - 您可以从主机服务提供商获取相关信息。 ** //
/** WordPress 的数据库名称，请更改 "database_name_here" */
define('DB_NAME', 'wordpress');
/** MySQL 数据库用户名称，请更改 "username_here" */
define('DB_USER', 'root');
/** MySQL 数据库密码，请更改 "password_here" */
define('DB_PASSWORD', 'Aa1234567');
/** MySQL 主机地址 */
define('DB_HOST', 'localhost');              //若非本机，则输入该服务器 IP 地址
/** 建立数据表时默认的文字编码 */
define('DB_CHARSET', 'utf8');
/** 数据库对照型态。如果不确定请勿更改。 */
define('DB_COLLATE', 'utf8_unicode_ci');
......中间省略......
/**
 * WordPress 本地化语言配置。默认为简体中文。
 *
 * 举例来说，要使用 WordPress 简体中文界面，只需要填入 'zh_CN'。
 * 更改此配置将 WordPress 本地化。对应的 MO 文件必须放置于 wp-content/languages 目录下。
 * 举例来说，将 zh_CN.mo 放置于 wp-content/languages 内并将 WPLANG 配置为'zh_CN'
 * 使用简体中文界面。
 */
define('WPLANG', 'zh_CN');                          //默认为简体中文 zh_CN
```



说明

WordPress配置文件中的文字若是乱码，将PuTTY选项的字符编码改为【Unicode UTF-8】。



WordPress配置完成后，必须重新启动Apache服务，配置才会生效。

```
[root@localhost wordpress]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

WordPress配置完成后，在浏览器中输入【http://IP地址/wordpress】，显示WordPress欢迎信息和配置选项，配置相关信息后，按【安装WordPress】。默认管理员账号为admin，可以依需求修改账号名称。

WORDPRESS

欢迎

欢迎使用著名的 WordPress 五分钟安装程序。如果您愿意花时间，可以看看介绍文档。或者只需简单地填写下面的表格，开始使用这个世界上最具扩展性、最强大的个人信息发布平台。

需要信息

您需要填写一些基本信息。无需担心填错，这些信息以后可以再次修改。

站点标题 Jerry_IT WordPress

用户名 admin
用户名只能包含字母、数字、空格、下划线、连字符（-）、句号和 @ 符号。

输入两次密码
若您留空密码栏，WordPress 将会为您生成一个密码。
•••••••
•••••••
中等
提示：您的密码最好至少包含 7 个字符。为了保证密码强度，使用大小写字母、数字和符号，例如 ! " ? $ % ^ & )。

您的电子邮件 jerry@jerryit.idv.cn
请仔细检查电子邮件地址后再继续。

隐私 允许搜索引擎对本站点进行索引。

WordPress安装完成后，系统显示使用以下账号和密码可以登录控制台。

成功！

WordPress 安装完成。您是否还沉浸在愉悦的安装过程中？很遗憾，一切皆已完成！ :)

用户名 admin

密码 *您设定的密码。*

登录

WordPress控制台登录界面为http://IP地址/wordpress/wp-login.php。



WordPress控制台界面为http://IP地址/wordpress/wp-admin/。




WordPress首页为http://IP地址/wordpress。



# 第31章

# 论坛——Discuz!

Discuz!官方网站:http://www.discuz.net/。

Discuz!是一款可免费下载的PHP社区论坛软件系统，简称DZ，由戴志康（Crossday）所创立，目前最新版本是7.2。前身为Crossday Bulletin（CDB），最初改自XMB，之后改写成为现在的Discuz! 社区论坛软件系统，由康盛创想所有。现在Discuz!已成为用户使用最多的社区论坛软件系统。

**使用层面：**

- 首页友情链接设置功能，可在首页直接切换隐身功能。
- 可在页面上直接切换模板风格，页面上方有导航栏。
- 版块区包含子分区、精华区、将主题表示高亮、彩色文字标题以及提高／降低主题位置的功能。
- 发表的文章可以在线编辑，也可以创建投票，发布商品、悬赏、活动、辩论等。
- 专属个人网页，可浏览自己的所有私人资料，如私人短信、论坛状态统计等。
- 卷标功能可将主题分门别类，并支持搜寻。卷标总表会在首页上显示。
- 论坛可以配置积分与虚拟金钱制度，可到“道具商店”用虚拟金钱来换取东西；积分影响到用户可以使用的功能与权限，可以购买文章，并可与其他会员互通有无。
- 边栏系统，具有高自由度自定义、高性能数据缓冲设计，内建许多常用边栏模块，包括会员排行、主题排行、附件展示、首页聚合等各种功能调用。

**管理层面：**

- 能在版块下再新增子版块。
- 可选择在注册程序中使用中文与动态化的验证码。
- 可选择让用户只能通过邀请码来注册的“邀请注册”功能。
- 能够只屏蔽单篇文章，可实现让会员无法观看但站务人员可观看单篇的功能，如有需要可再进行解除或删除的处理。

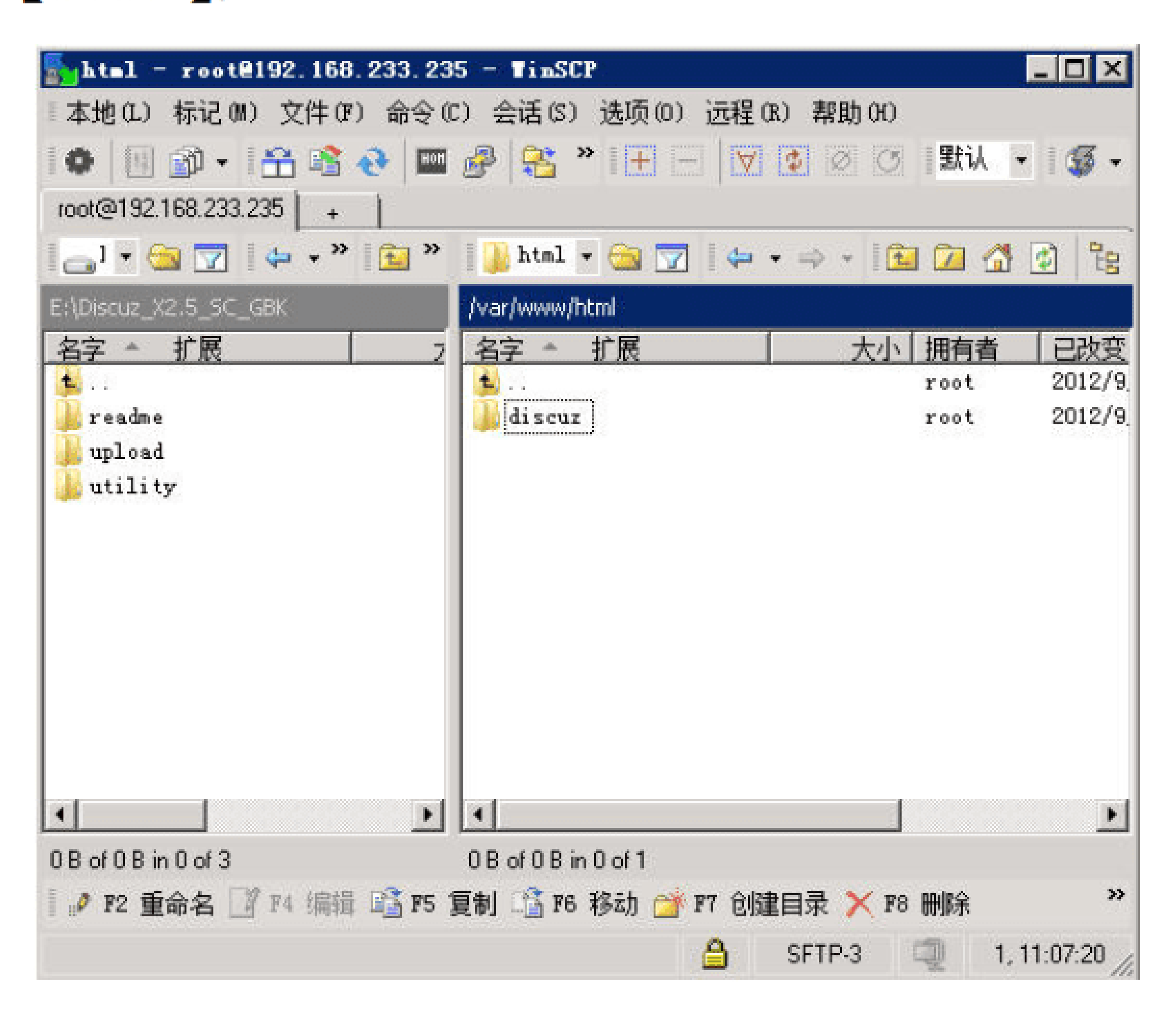
- 版主可以将好文章的链接加入到版块的上方，与置顶不同的是，这并不会影响浏览主题的空间，较为节省空间。
- 系统管理与个人配置页面也清楚地分门别类，以便进行详细配置。可以自由配置好友名单、控制面板。
- 结合了电子商务的功能，可以自己开设虚拟店面，并有交易明细、信用评价的功能与机制。

**架构层面：**

- 大量运用AJAX以加快使用流程。
- 内建多种模板风格，风格系统模板化，有可视化编辑器，并可进行一键安装或移除风格、插件。
- 以PHP为核心，具有跨平台特性，可使用Apache（或Microsoft Windows中的IIS）配合MySQL运行Discuz!。
- 可与插件整合，如SupeSite、X-Space、SiteEngine、ShopEx等，可在论坛中使用，也可只在管理界面中使用。
- 可对于论坛程序以及模板进行扩充。

## 31.1 Discuz!软件安装前的配置

参考LAMP建站软件需求将LAMP环境安装好，然后将Discuz!软件上传到LAMP服务器，可以利用WinSCP工具将Discuz!软件的upload目录上传到Apache网页目录（/var/www/html）下，并将文件夹重命名为【discuz】。




检查Apache配置文件是否支持UTF-8编码，如果不支持UTF-8编码，则修改成UTF-8。创建一个名称为【discuz】的数据库供Discuz!系统使用，如果不知道如何创建数据库，可以参考LAMP建站软件需求，来创建Discuz!所需的数据库。

## 31.2 安装Discuz!软件

安装Discuz!软件前，必须进行配置，首先进入Discuz!目录，复制默认全局配置文件config_global_default.php并重命名为config_global.php，再复制config_ucenter_default.php配置文件并重命名为config_ucenter.php，然后将config、data、uc_server目录权限设置为777，另外也将uc_client/data/cache的目录权限设置为777。

```
[root@localhost ~]# cd /var/www/html/Discuz!  //进入Discuz!目录
[root@localhost Discuz!]# cp config/config_global_default.php  config/config_global.php
            //复制配置文件并重命名
[root@localhost Discuz!]# cp config/config_ucenter_default.php config/config_ucenter.php
            //复制配置文件并重命名
[root@localhost Discuz!]# chmod 777 -R config data uc_server
[root@localhost Discuz!]# chmod 777 uc_client/data/cache
```

配置完成后，在浏览器中输入【http://IP地址/Discuz!/install/】，显示安装向导，提示是否接受中文版授权协议，按【我同意】继续安装，按【我不同意】即结束安装。




相关环境配置后，就该配置目录权限了。




安装环境必须符合所有条件，将相关文件及目录权限配置为777。

```
[root@localhost ~]# cd /var/www/html/Discuz!
[root@localhost Discuz!]# chmod 777 config.inc.php attachments forumdata forumdata/cache
forumdata/templates  forumdata/threadcaches  forumdata/logs  uc_client/data/cache
```

权限配置完毕后，重新刷新Discuz!网页，显示当前状态即为可写。

| 目录文件 | 所需状态 | 当前状态 |
|---|---|---|
| ./config/config_global.php | 可写 | 可写 |
| ./config/config_ucenter.php | 可写 | 可写 |
| ./config | 可写 | 可写 |
| ./data | 可写 | 可写 |
| ./data/cache | 可写 | 可写 |
| ./data/avatar | 可写 | 可写 |
| ./data/plugindata | 可写 | 可写 |
| ./data/download | 可写 | 可写 |
| ./data/addonmd5 | 可写 | 可写 |
| ./data/template | 可写 | 可写 |
| ./data/threadcache | 可写 | 可写 |
| ./data/attachment | 可写 | 可写 |
| ./data/attachment/album | 可写 | 可写 |
| ./data/attachment/forum | 可写 | 可写 |
| ./data/attachment/group | 可写 | 可写 |
| ./data/log | 可写 | 可写 |
| ./uc_client/data/cache | 可写 | 可写 |
| ./uc_server/data/ | 可写 | 可写 |
| ./uc_server/data/cache | 可写 | 可写 |
| ./uc_server/data/avatar | 可写 | 可写 |
| ./uc_server/data/backup | 可写 | 可写 |
| ./uc_server/data/logs | 可写 | 可写 |
| ./uc_server/data/tmp | 可写 | 可写 |
| ./uc_server/data/view | 可写 | 可写 |

设置运行环境，此处为全新安装，所以选择【全新安装Discuz!X（含UCenter Server）】，按【下一步】。




在【安装数据库】选项中，数据库服务器就是MySQL数据库服务器，默认为localhost，除非是其他的数据库服务器，否则不修改。数据库名为Discuz!所使用的数据库，数据库用户名和密码则输入拥有Discuz!数据库的账号和密码，其他使用默认配置。



配置Discuz!管理员账号默认为admin，配置管理员密码及E-mail，配置完成后，按【下一步】。

填写管理员信息

管理员账号: admin
管理员密码: ••••••••• 管理员密码不能为空
重复密码: •••••••••
管理员 Email: admin@comsenz.com
附加数据: 完整地区数据（四级）
开启门户功能:
开启家园功能:
开启群组功能:
下一步

开始创建数据库，在数据库安装过程中，请勿关闭浏览器以免安装失败。




数据库安装成功后，安装向导提示安装成功。




若可以打开Discuz!首页的话，记得将Install安装目录改名或删除。

```
[root@localhost Discuz!]# mv install install_old
```

在浏览器中输入【http://IP地址/Discuz!】，打开Discuz！首页，下图所示为Discuz！默认版面，可以进入管理员管理中心去配置。




输入用户账号和密码，Discuz!安装完成后只有管理员账号，如果注册了其他用户，可以使用其他用户登录。在用户个人中心，配置账户信息。



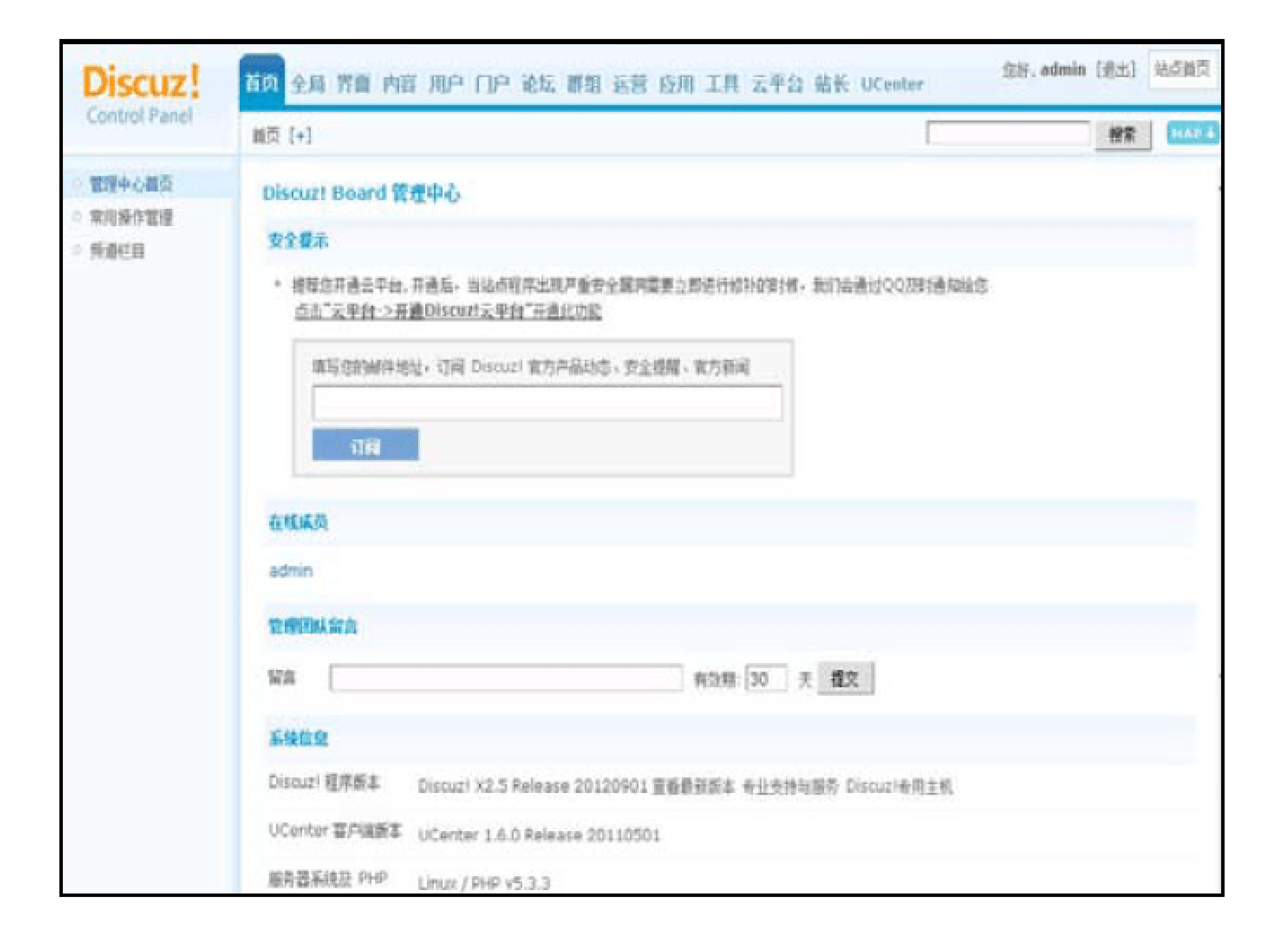




在Discuz!管理员管理中心，打开浏览器，输入【http://IP地址/Discuz!/admincp.php】，然后输入管理员账号和密码。




登录管理员管理中心后，请依需求修改，这里不再多说。


Discuz!
Control Panel
首页 全局 界面 内容 用户 门户 论坛 群组 运营 应用 工具 云平台 站长 UCenter
您好，admin [退出] 站点首页
首页 [+]
搜索
管理中心首页
常用操作管理
频道栏目
Discuz! Board 管理中心
安全提示
点击"云平台->开通Discuz!云平台"开通此功能
填写您的邮件地址，订阅 Discuz! 官方产品动态、安全提醒、官方新闻
订阅
在线成员
admin
管理团队留言
留言
有效期: 30 天 提交
系统信息
Discuz! 程序版本 Discuz! X2.5 Release 20120901
UCenter 客户端版本 UCenter 1.6.0 Release 20110501
服务器系统及 PHP Linux / PHP v5.3.3

# 第32章

# 百科——MediaWiki

MediaWiki官方网站：http://www.mediawiki.org/wiki/Download/zh-hans。

你可能知道维基百科这部自由的百科全书，但可能对一些相似但是不同的名词感到困惑，如维基（Wiki）、维基百科（Wikipedia）、维基媒体（Wikimedia）、MediaWiki 或MediaZilla。

MediaWiki是一个运行在服务器端的自由软件，基于GNU General Public License（GPL协议）发行。它能够平稳地运行在日访问量上百万的网站服务器集群中。MediaWiki是一个强大、可扩展、功能丰富的维基软件，它使用PHP技术来访问和显示存储在MySQL数据库中的数据。

使用MediaWiki的维基文本格式，用户不懂得XHTML或CSS也可以很容易地编辑内容。

当一个用户提交一个编辑给一个页面时，MediaWiki会将它写入数据库，但是不会删除这个页面的先前版本，这使得页面遭到故意破坏或垃圾信息干扰时可以快速恢复。MediaWiki也可以管理图像和多媒体文件，这些文件存储在文件系统中。对于拥有大量用户的大型维基站点，MediaWiki支持缓存，并且可以很容易地添加Squid代理服务器软件。

## 32.1 MediaWiki软件安装前的配置

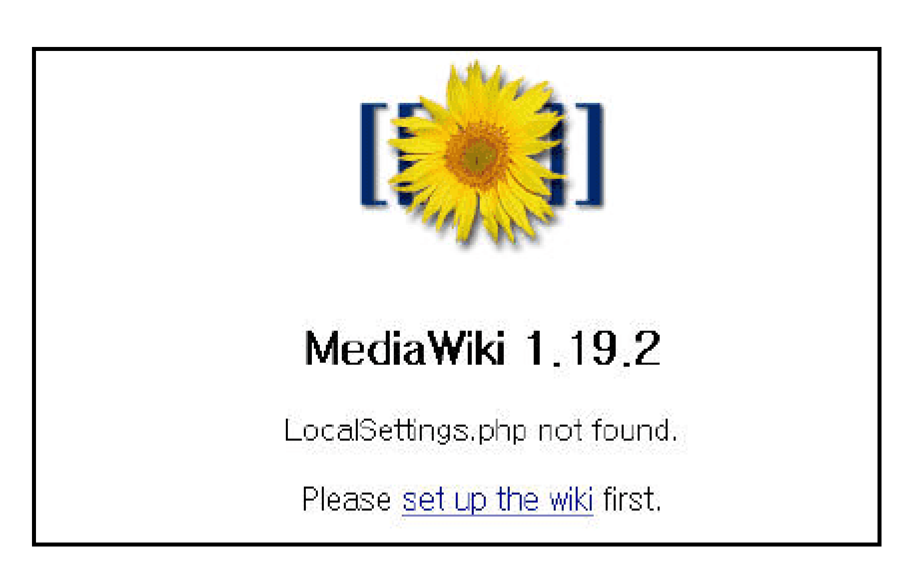
参考LAMP建站软件需求将LAMP环境安装好，再创建一个名称为【mediawiki】的数据库供MediaWiki使用，如果不知道如何创建数据库，可以参考LAMP建站软件，来创建MediaWiki所需的数据库。

使用wget命令方式下载MediaWiki软件，然后解压缩MediaWiki软件，将解压缩后的MediaWiki目录复制至Apache网页目录下，并将目录权限设置为apache。

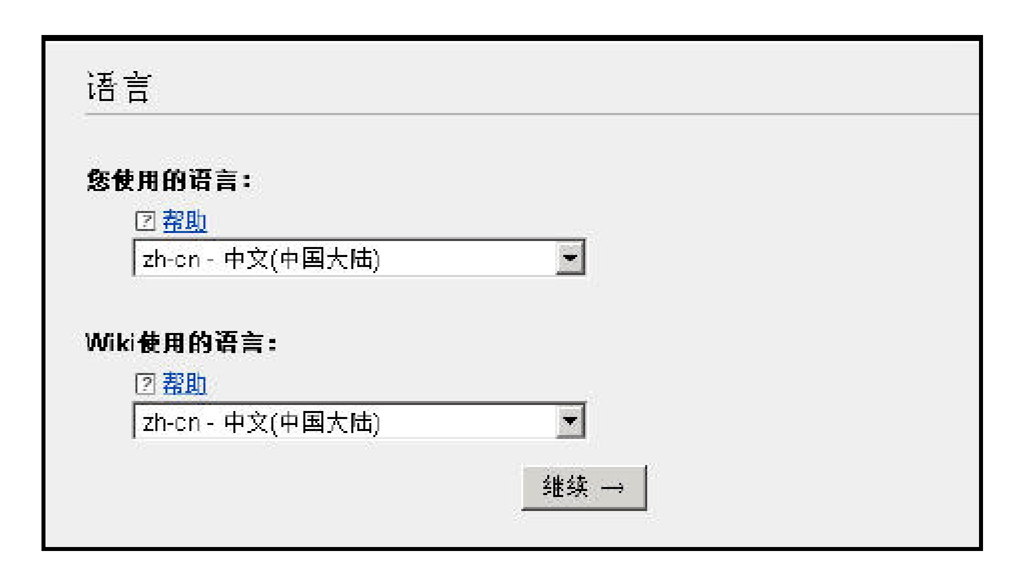
```
[root@localhost ~]# wget
http://download.wikimedia.org/mediawiki/1.19/mediawiki-1.19.2.tar.gz
…中间省略…
[root@localhost ~]# tar -zxvf mediawiki-1.19.2.tar.gz
…中间省略…
[root@localhost ~]# mv mediawiki-1.19.2 /var/www/html/mediawiki
[root@localhost ~]# chown -R apache. /var/www/html/mediawiki
```

## 32.2 安装MediaWiki软件

在浏览器中输入【http://IP地址地址/mediawiki】，MediaWiki安装程序会提示没有LocalSettings.php文件，所以不能安装MediaWiki软件，单击【set up the wiki】进入MediaWiki安装程序。




在MediaWiki安装程序中配置语言，默认会根据系统及浏览器语言自动选择，如果确定无误，按【继续】。

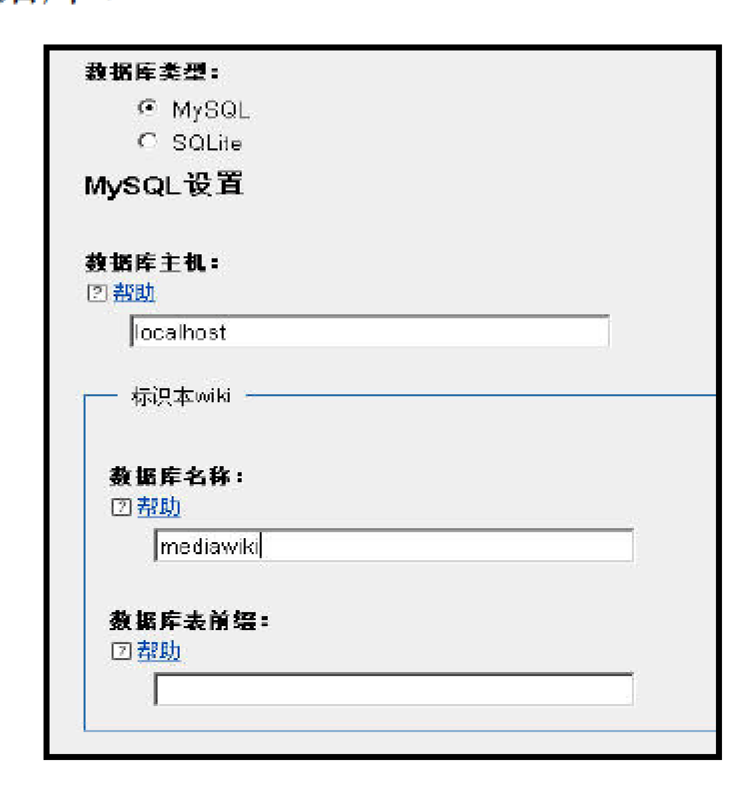



下面是MediaWiki安装程序欢迎界面，阅读完毕后，按【继续】。

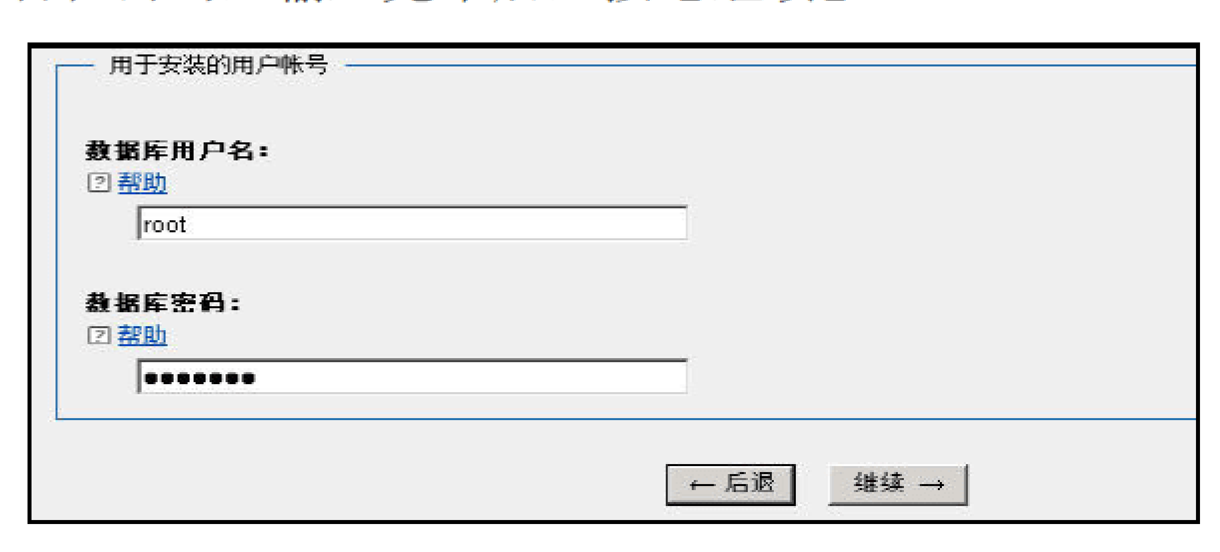



在MediaWiki安装程序中配置数据库类型，默认使用MySQL，数据库服务器位置默认为localhost本机，如果MySQL数据库服务器为其他主机，请修改为数据库服务器的IP地址，并开

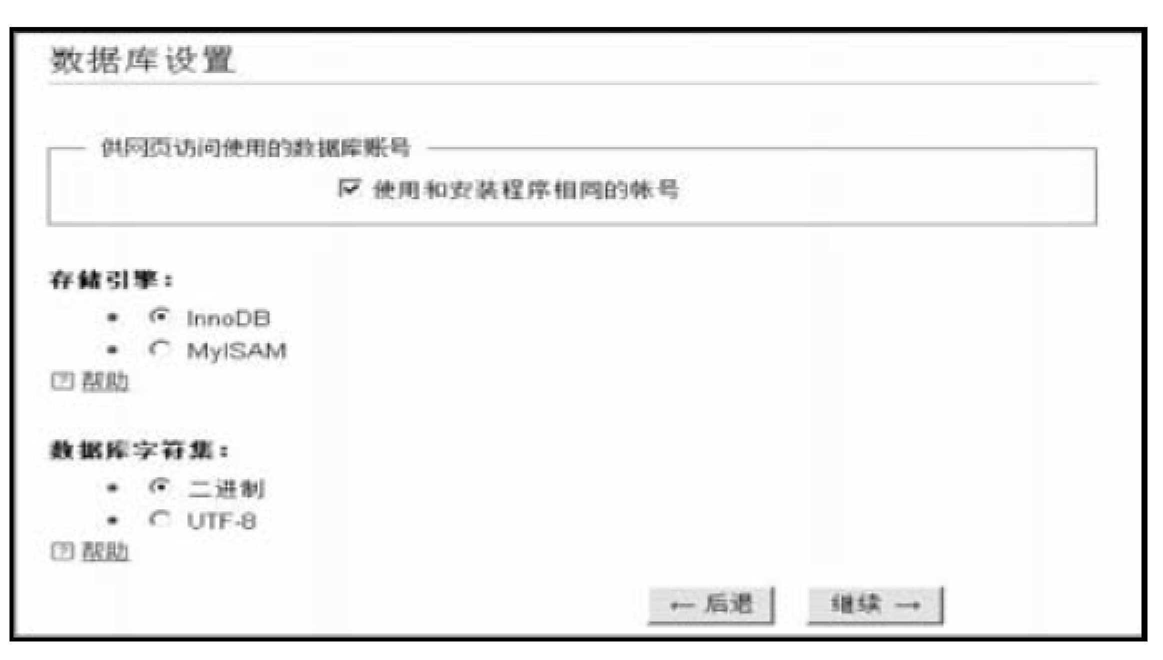
放3306端口，以免无法连接数据库。



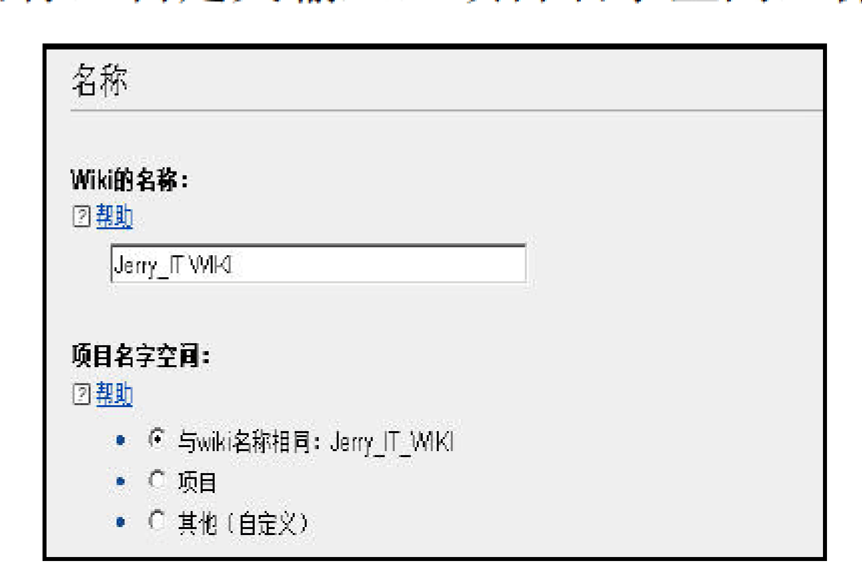

配置数据库用户名和密码，输入完毕后，按【继续】。




在【数据库设置】的【供网页访问使用的数据库账号】中，勾选【使用和安装程序相同的账号】，其他配置保留默认选项，按【继续】。




配置MediaWiki网站的名称，自定义输入，项目名字空间，保留默认。



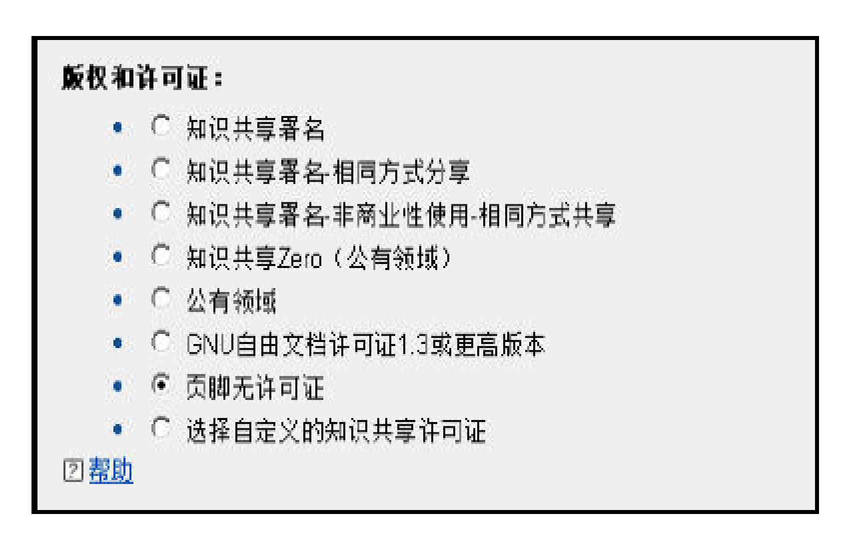

配置MediaWiki网站管理员账号和密码，自定义输入，到这一步其实就可以完成安装了，不过这里继续介绍高级配置，所以选择【多问我一些问题吧。】，按【继续】。



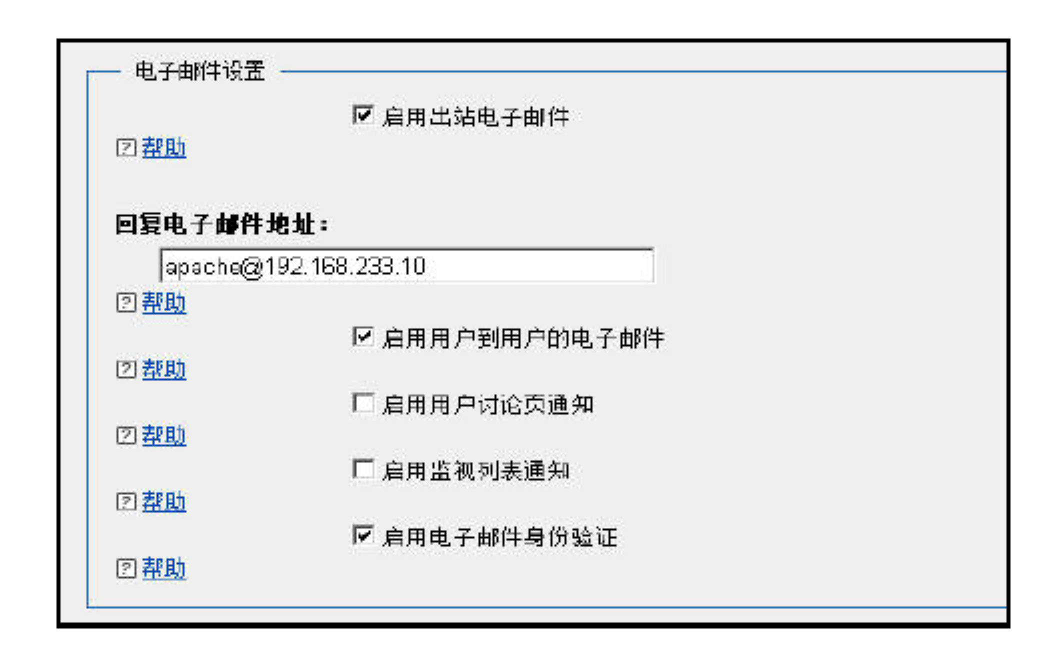

客户端权限配置，默认为【传统wiki】代表所有人都可以编辑，包含未注册的用户，建议配置为【需要注册账号】。




版权和许可证默认使用【页脚无许可证】。



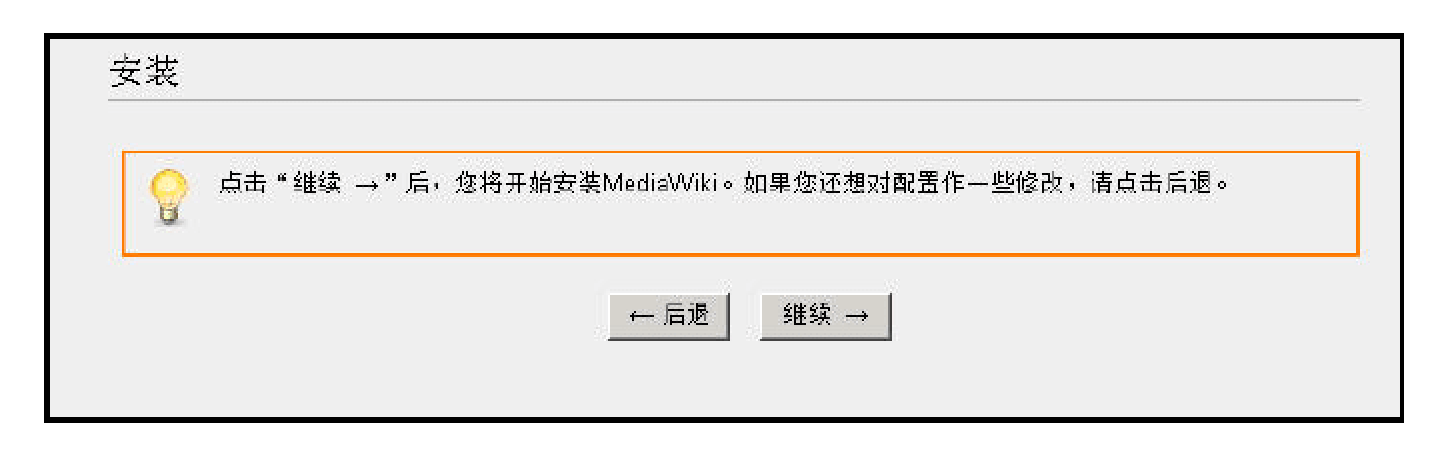

配置是否启用出站电子邮件，默认一定不是所要使用的电子邮件，先保留默认，待安装完后再进行配置。



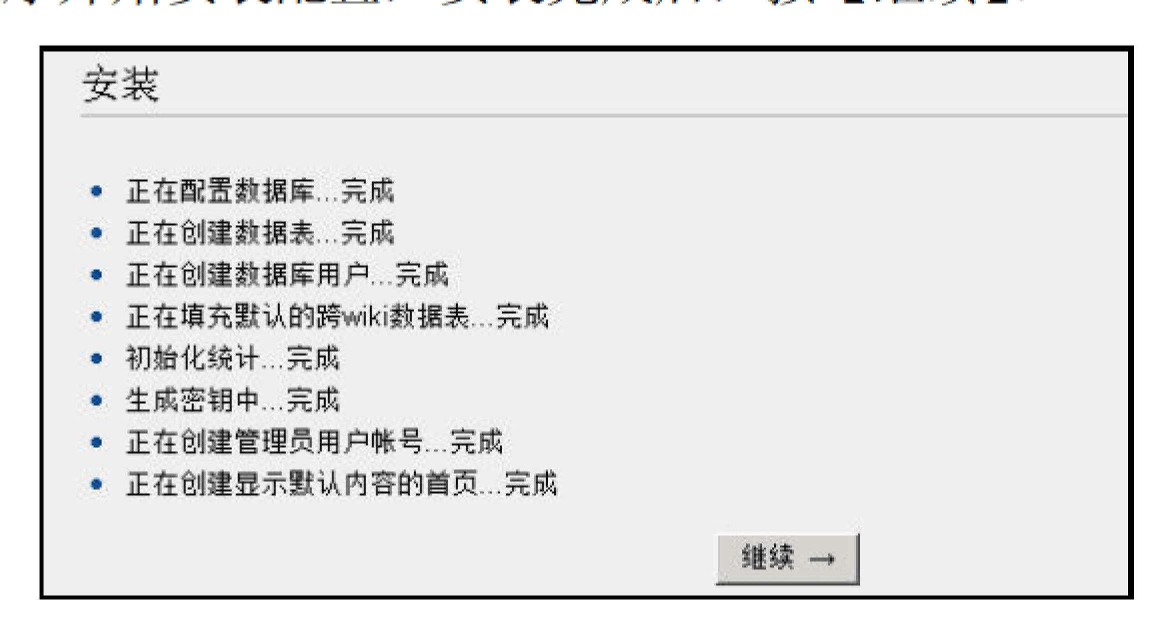
图片和文件上传，默认不启用文件上传，可依需求情况启用，按【继续】。




一切配置完成后，安装程序会进行安装前的最后确认，确认无误后，按【继续】。



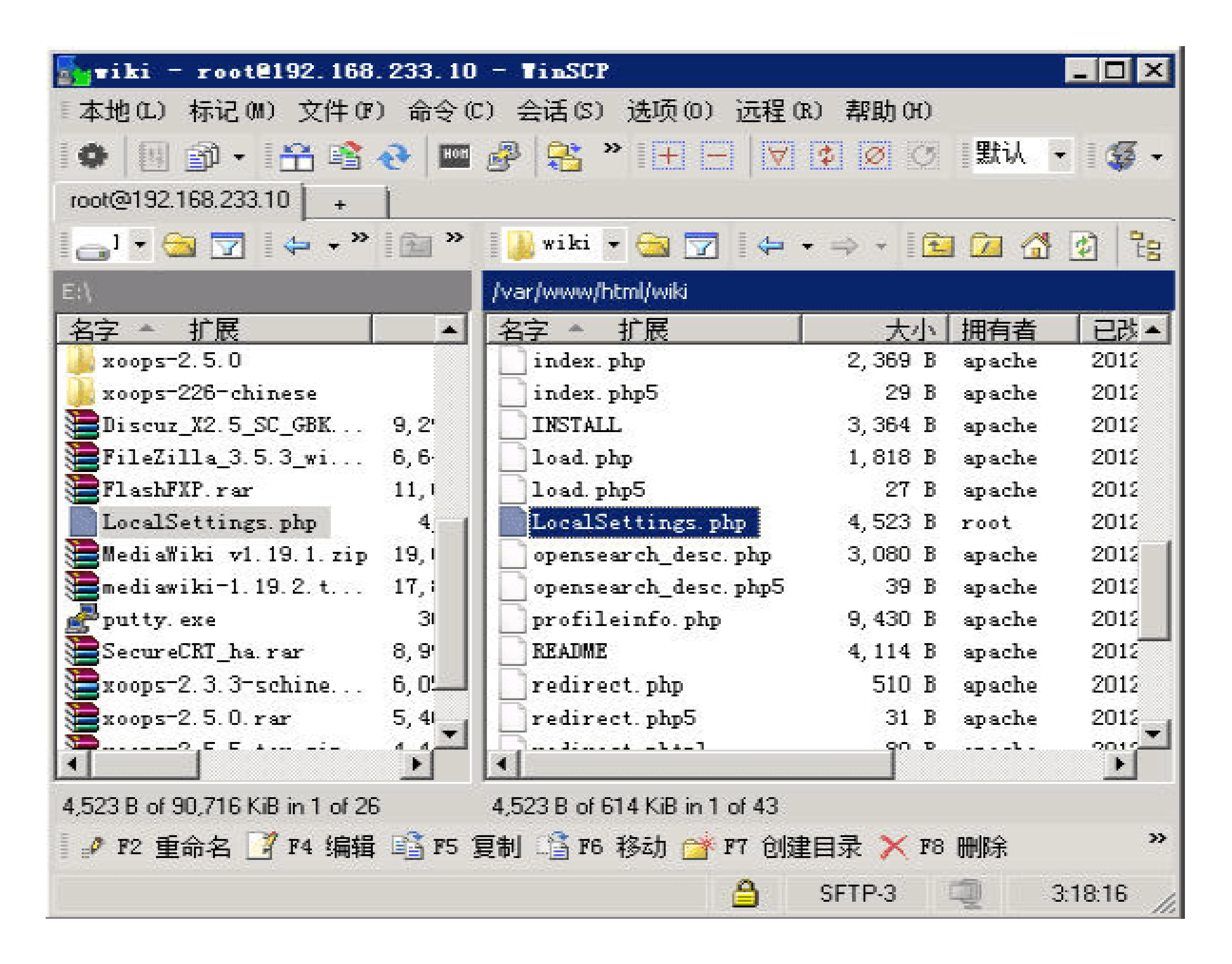

MediaWiki安装程序开始安装配置，安装完成后，按【继续】。




安装完成后，MediaWiki安装程序会产生一个LocalSettings.php文件，提示需要下载，此文件为MediaWiki网站的配置文件，所以先下载到本机硬盘上。




下载MediaWiki配置文件后，利用WinSCP工具将文件上传到MediaWiki网站目录。



然后回到MediaWiki安装程序，进入Wiki，如下所示，代表安装完成。



按右上角的【登录/创建账户】，一开始只能使用管理员账号和密码登录，输入完毕后，按【登录】。




登录后，MediaWiki首页右上角就会显示选项，可以进行配置，有关详细配置可以自行摸索。



# 第六部分

# 附录篇



# 附录A

# VMware Player 4——创建CentOS练习环境

VMware Player官方网站：http://www.vmware.com/products/player/overv.ew.html。

VMware Player是一款可免费下载的虚拟化软件，以往版本只具有开启虚拟机的功能，到第三版时可以建立虚拟机，如今VirtualBox、Hyper-V Server等虚拟化产品陆续推出免费版本，这算是VMware的重大突破，VMware宣称优于Windows 7 XP mode，可见VMware感觉免费使用已渐渐影响到虚拟化市场的占有有率，VMware Player可以支持Windows 7系统（含Host跟Guest OS）及OpenGL功能，支持32/64位操作系统，4个CPU及32GB内存。

## 下载VMware Player 4需知

以前需要注册免费账号后才可以下载，申请账号时需要企业的电子邮件，条件比较严格，免费信箱都不可以注册，不过后来可以接受使用hotmail注册，申请注册完成后，就可以开始下载了，选择for 32-bit and 64-bit Windows下载。



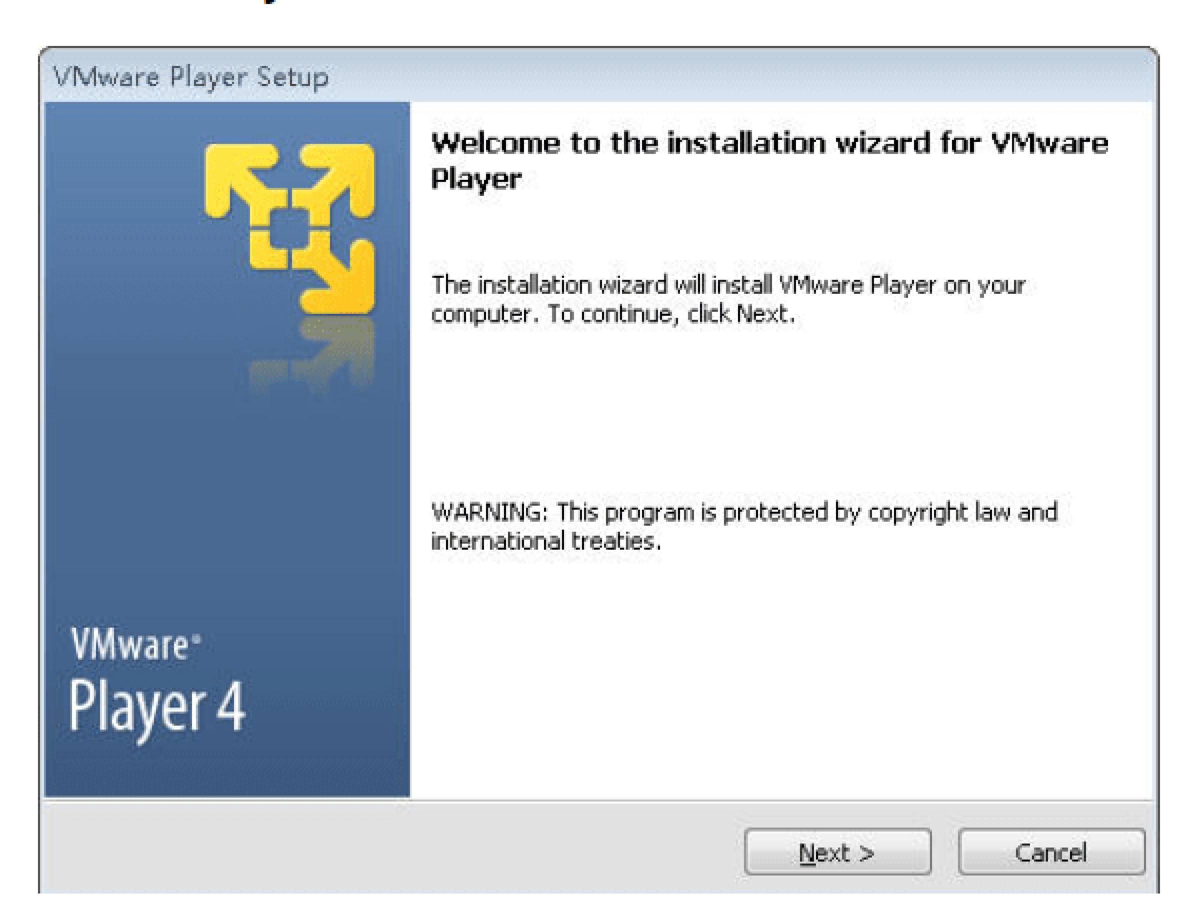

介绍使用VMware Player虚拟化软件，是为了方便大家在安装VMware Player后，可以将CentOS操作系统安装在VMware Player虚拟机上，这样就不用将CentOS操作系统安装在另一台实体计算机上，只要使用少量的资源就可以运行CentOS操作系统，练习使用CentOS起来就更加得心应手。

## VMware Player 4安装步骤

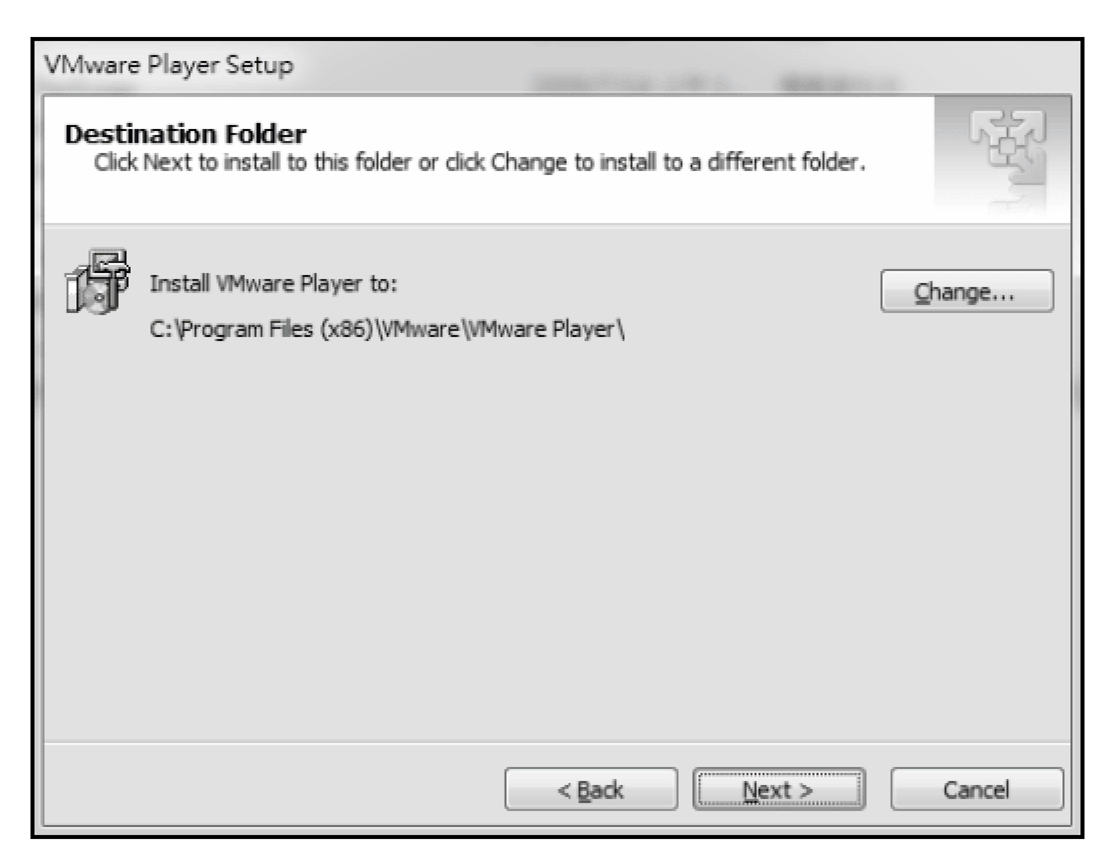
步骤01　下载VMware Player 4安装文件后，选择VMware Player 4执行程序进行安装。



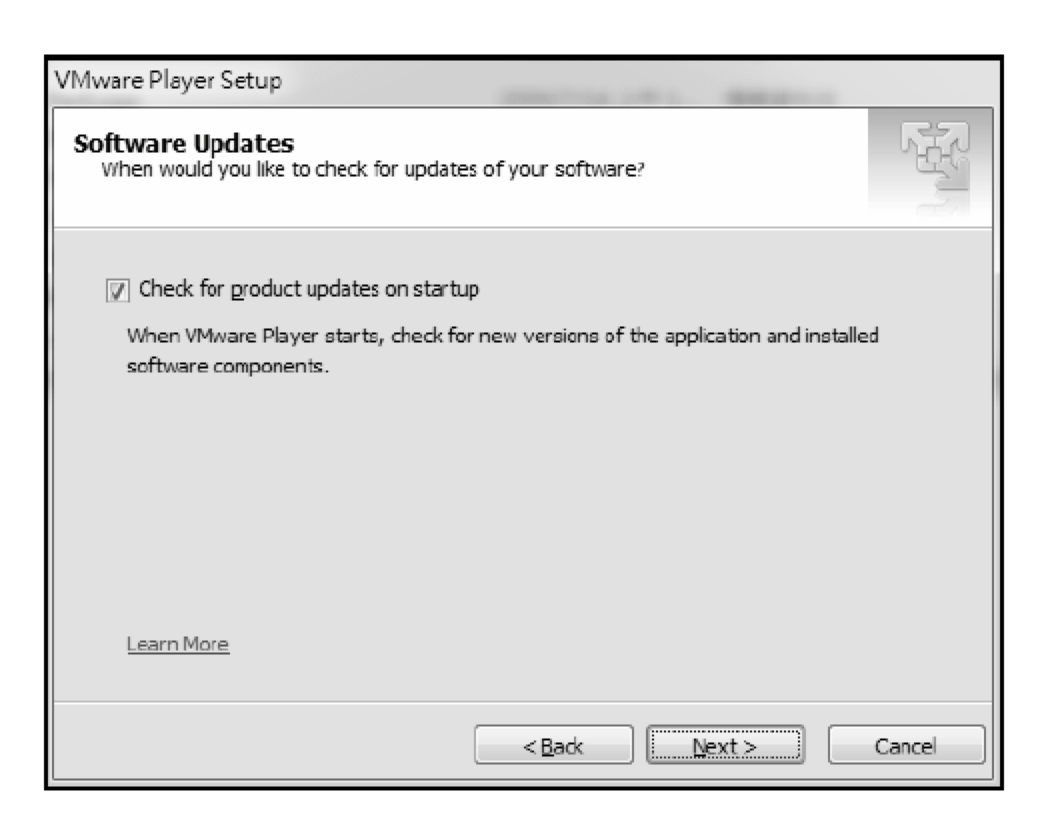

步骤02 出现VMware Player 4欢迎安装画面，单击【Next】。



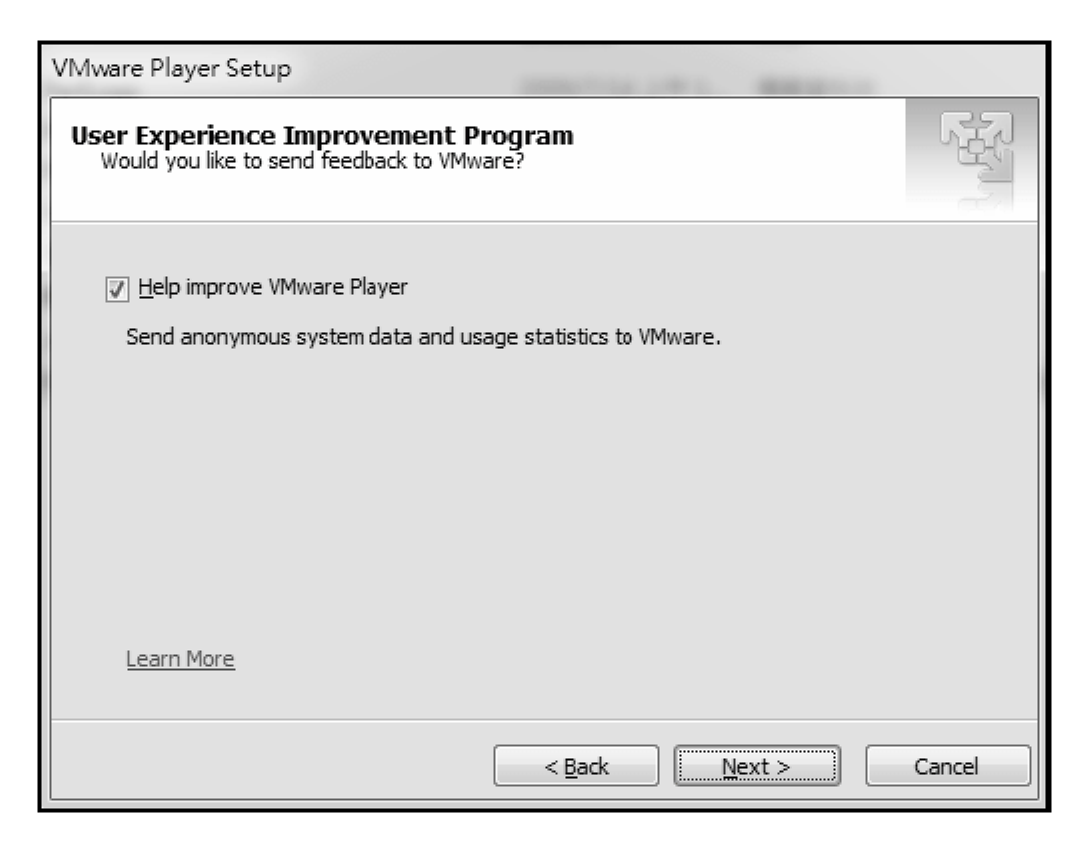

步骤03 选择VMware Player 4的安装路径，建议不要修改，如果需要修改路径，单击【Change】，确定好安装路径后，按【Next】。



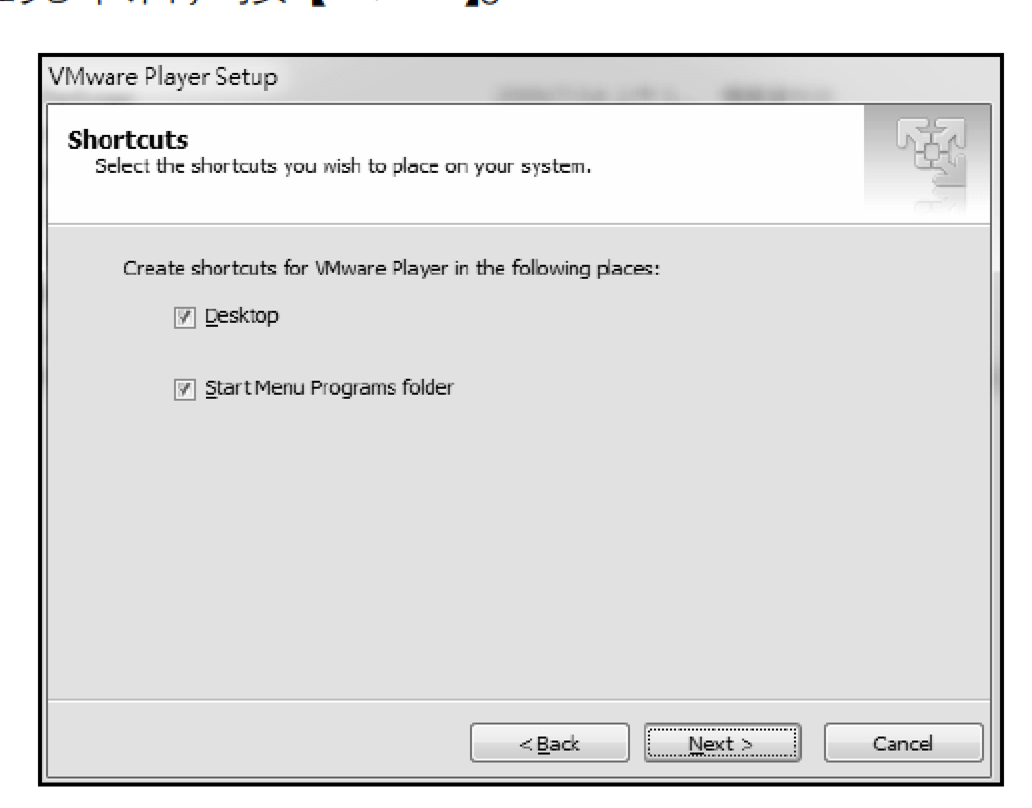

步骤04 提示开始运行软件的时候是否检查新版本，默认勾选【Check for product updates on startup】，按【Next】。



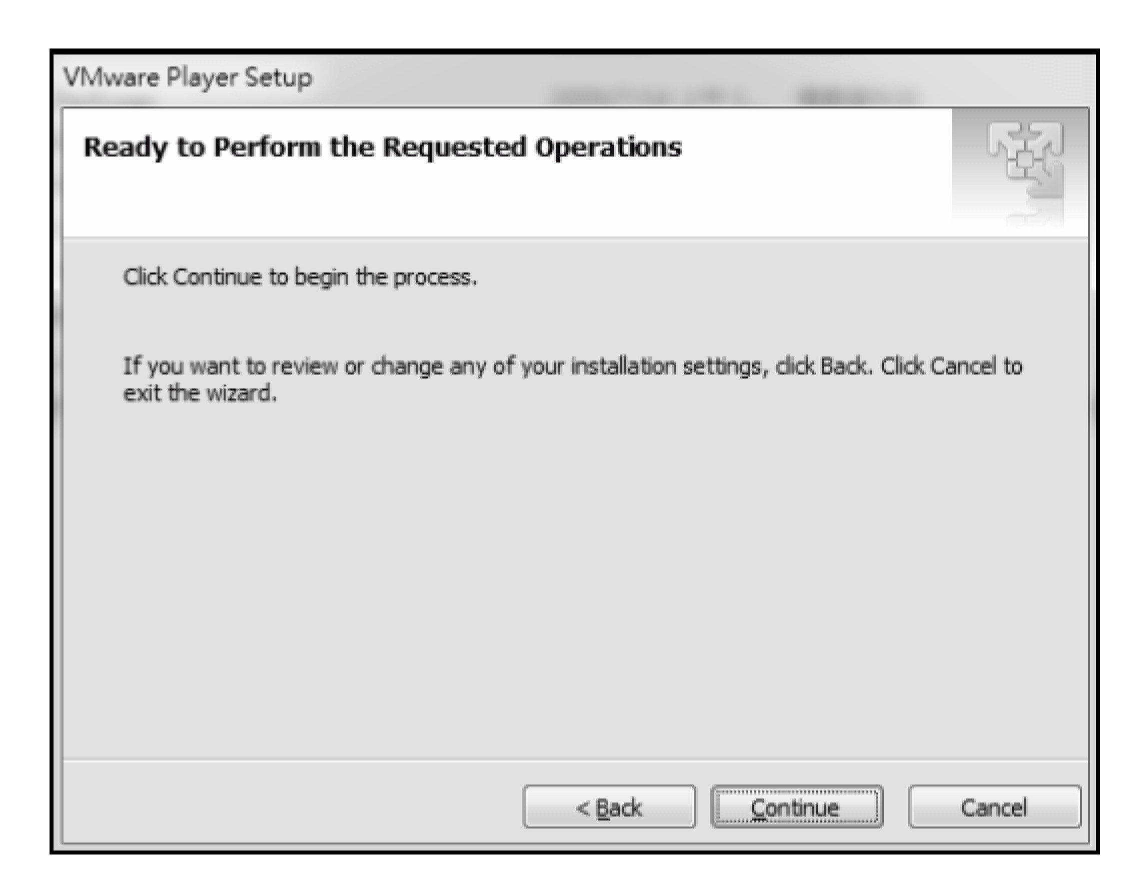

步骤05 提示用户是否体验改善计划，默认勾选【Help improve VMware Player】，按【Next】。



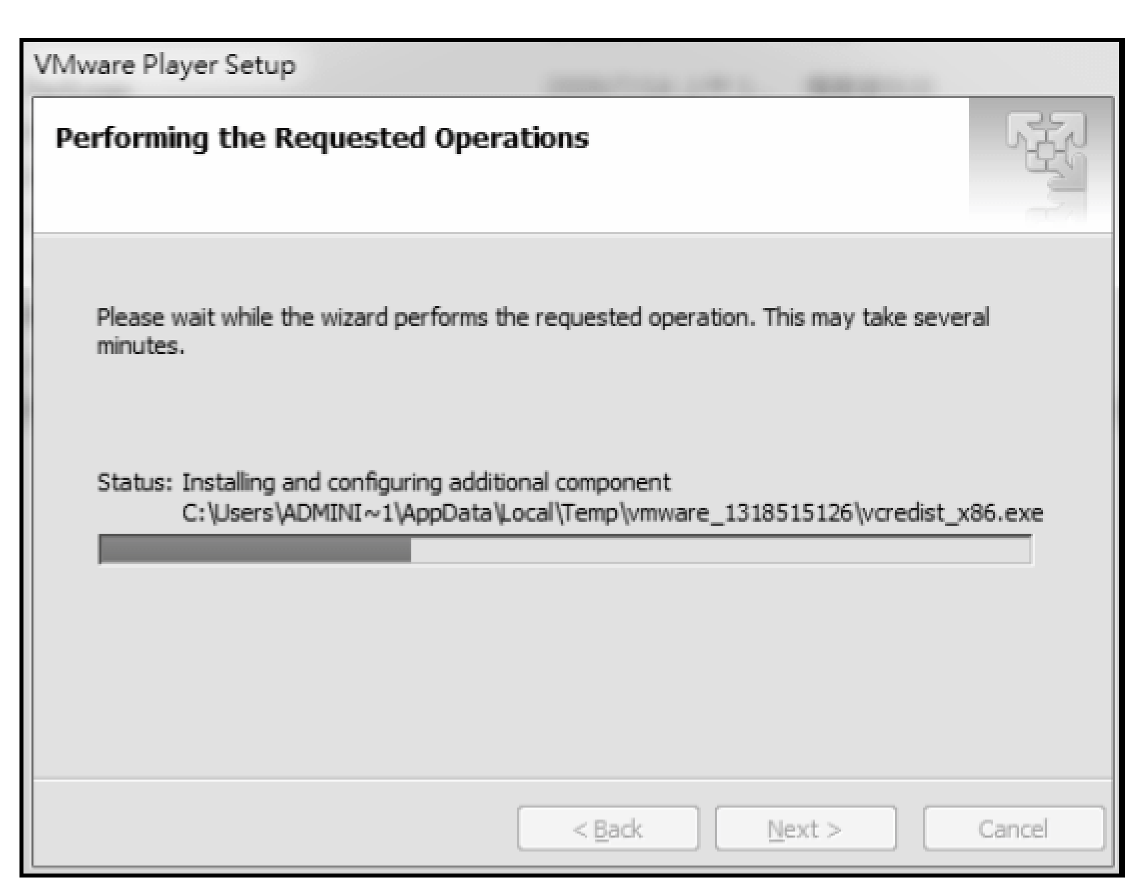

步骤06 提示创建VMware Player软件快捷方式的位置，可以创建于桌面（Desktop）、开始菜单程序文件夹（Start Menu Programs folder），默认全选，可根据需求勾选，设置完毕后，按【Next】。




步骤07 提示安装VMware Player的过程没有任何问题，按【Continue】进行安装。




步骤08 VMware Player安装正在进行。




步骤09 VMware Player安装完成后，会要求重新启动，建议立即重新启动，这样VMware Player安装配置才可以生效，按【Restart Now】。




**说明**

注意，若计算机中有安装还原设备，请稍后重新启动，按【Restart Later】，VMware Player还可以运行。

步骤10 VMware Player安装完成后，会在计算机中增加两块VMware虚拟网卡【VMnet1】及【VMnet8】，如下图所示。




## 创建虚拟机

下面介绍该如何创建一个虚拟机，以便安装CentOS操作系统。

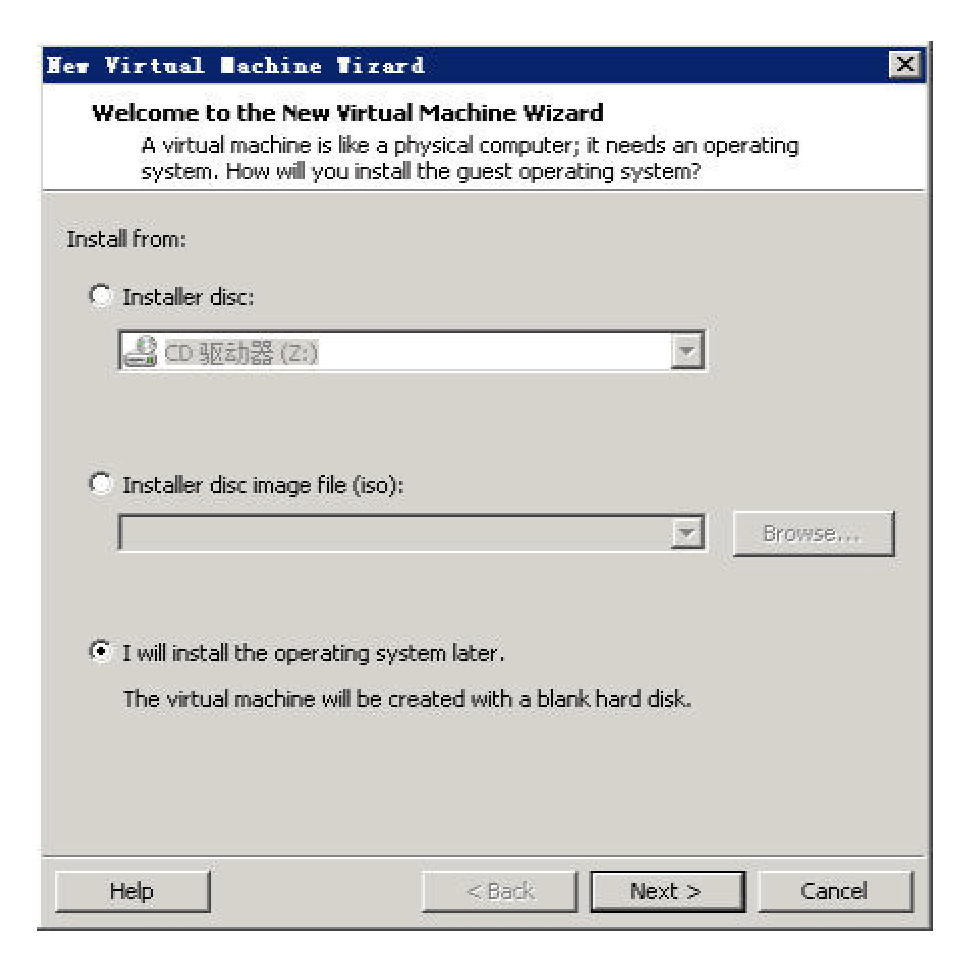
步骤01 VMware Player 4第一次开启时会出现License Agreement授权询问，选择【Yes,I accept the terms in the license agreement】，再按【OK】。



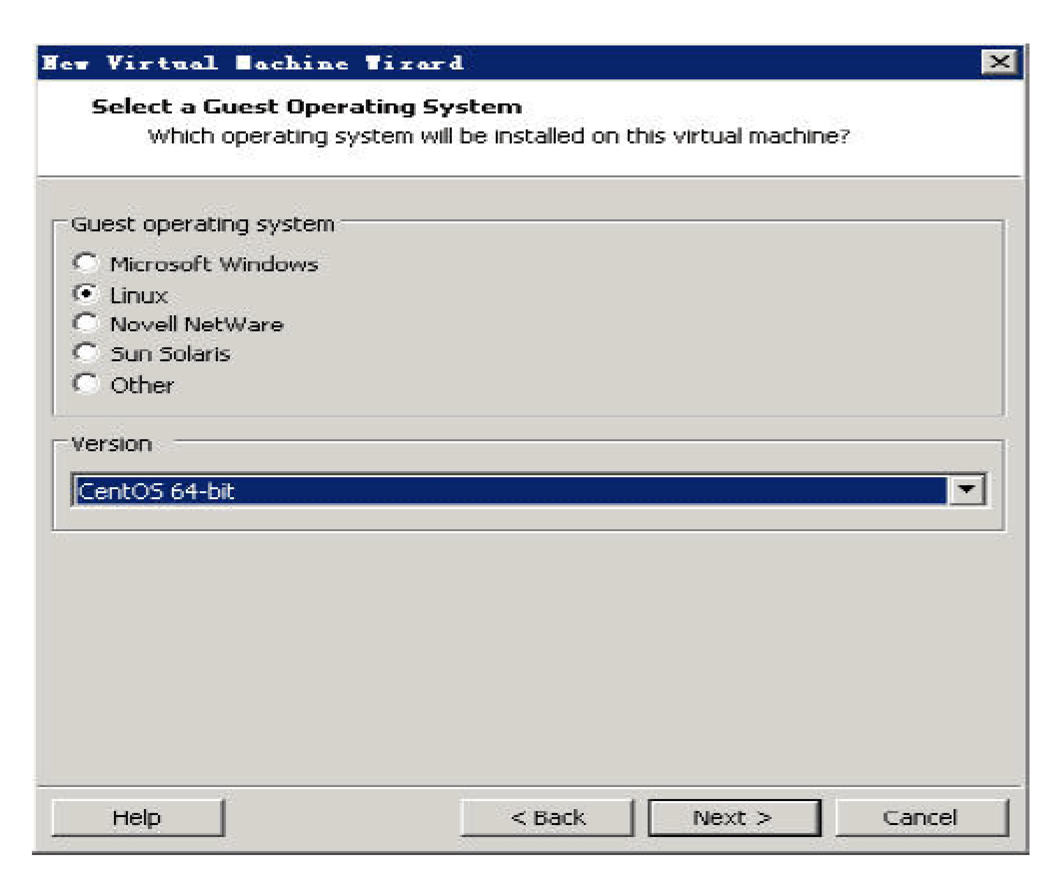

步骤02 显示VMware Player 4窗口，目前没有创建任何虚拟机，按【Create a New Virtual Machine】创建新的虚拟机。



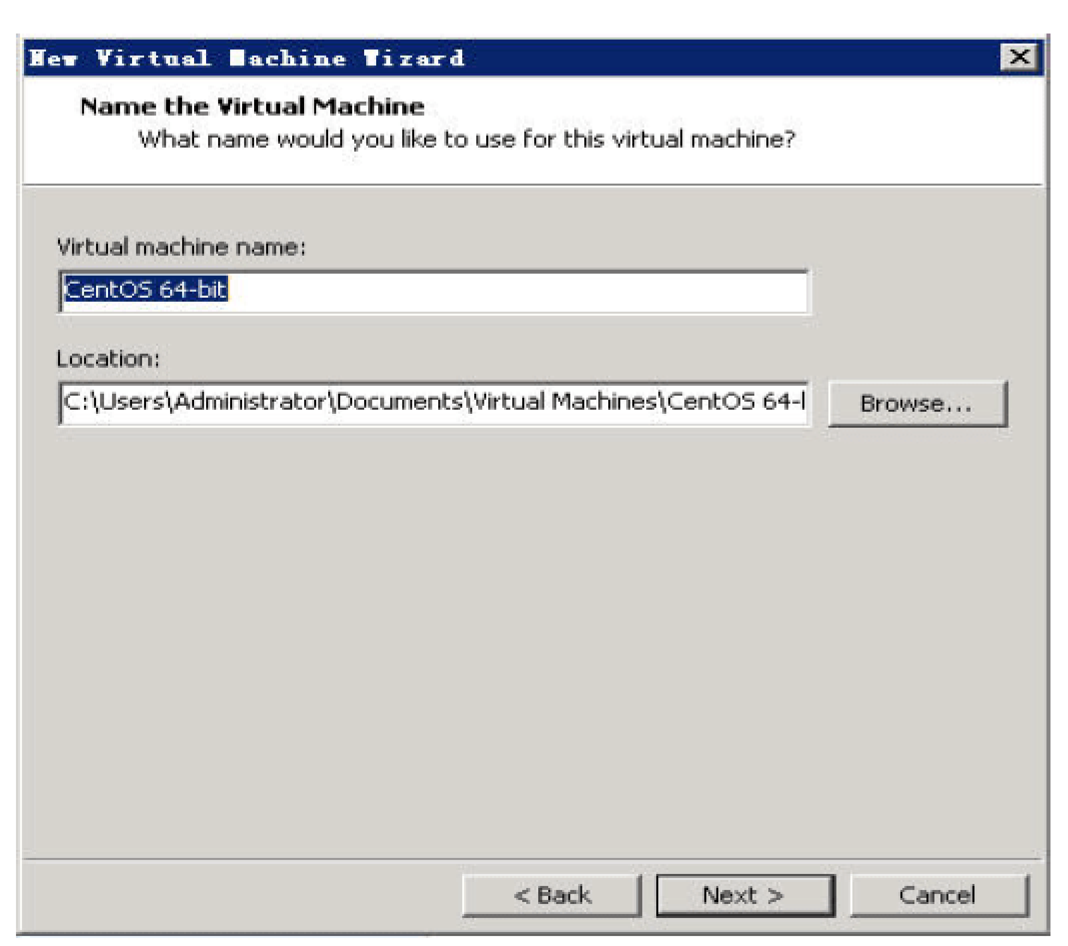

步骤03 开始创建虚拟机时要选择安装文件来源，可以使用光驱或者ISO文件安装，先不选择任何安装来源，待建立完成后再进行设置，选择【I will install the operating system later】，按【Next】。



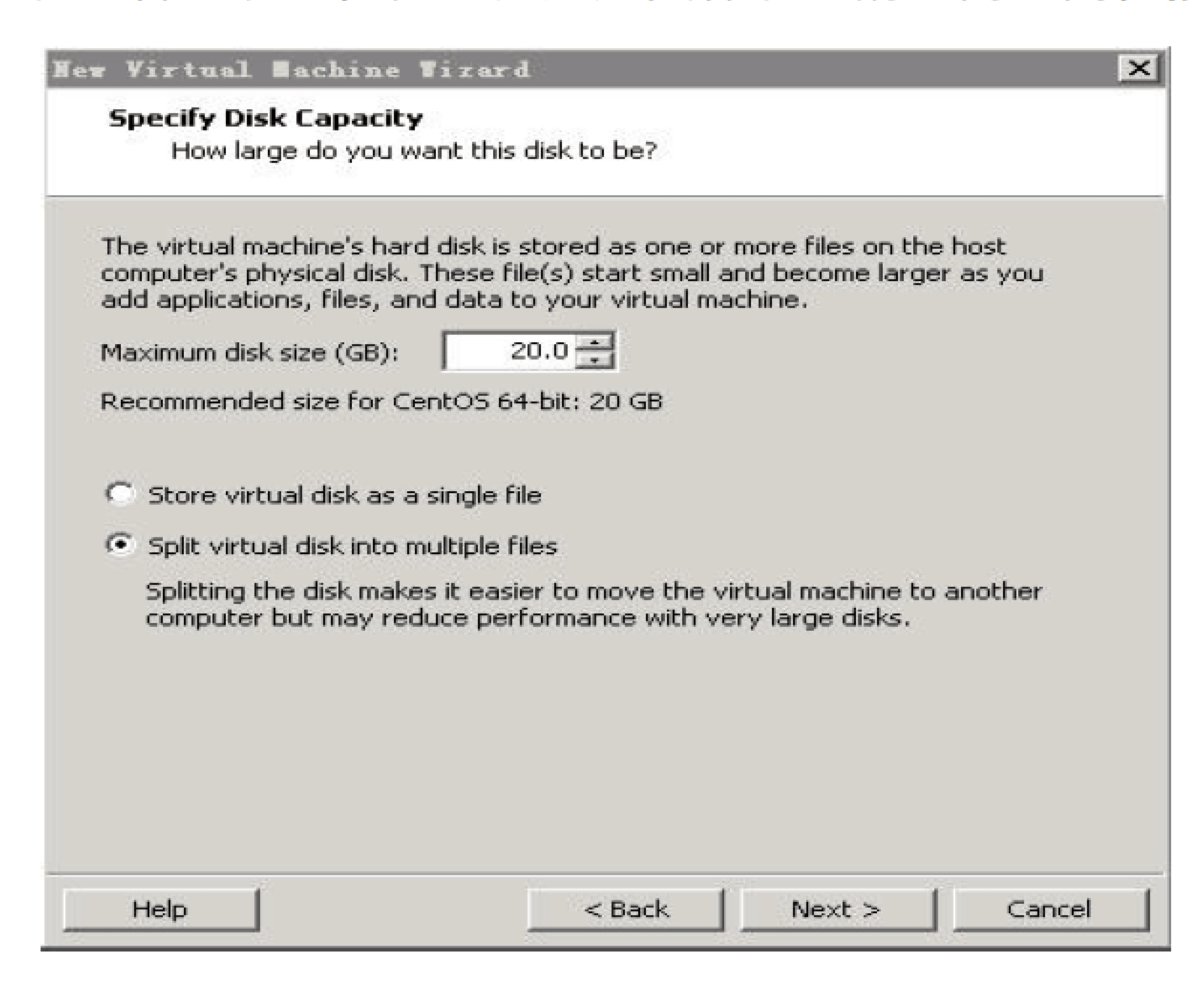

步骤 04 选择操作系统类型【Linux】后，由于要安装CentOS x86_64，所以【Version】选择【CentOS 64-bit】，按【Next】。



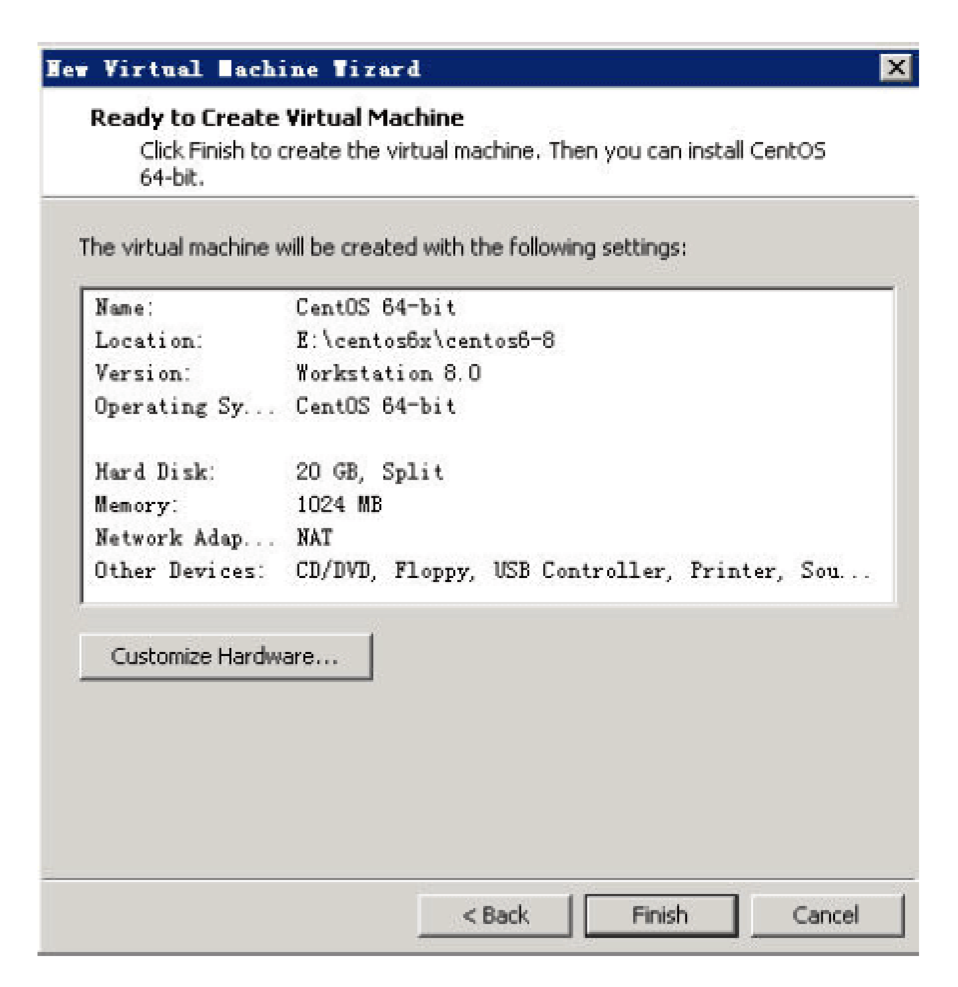

步骤 05 输入虚拟机的名称，存放路径也会依所输入的虚拟机名称而改变，存储目录建议尽量放置在不同的硬盘上，效果也比较好一点，设置完成后，按【Next】。



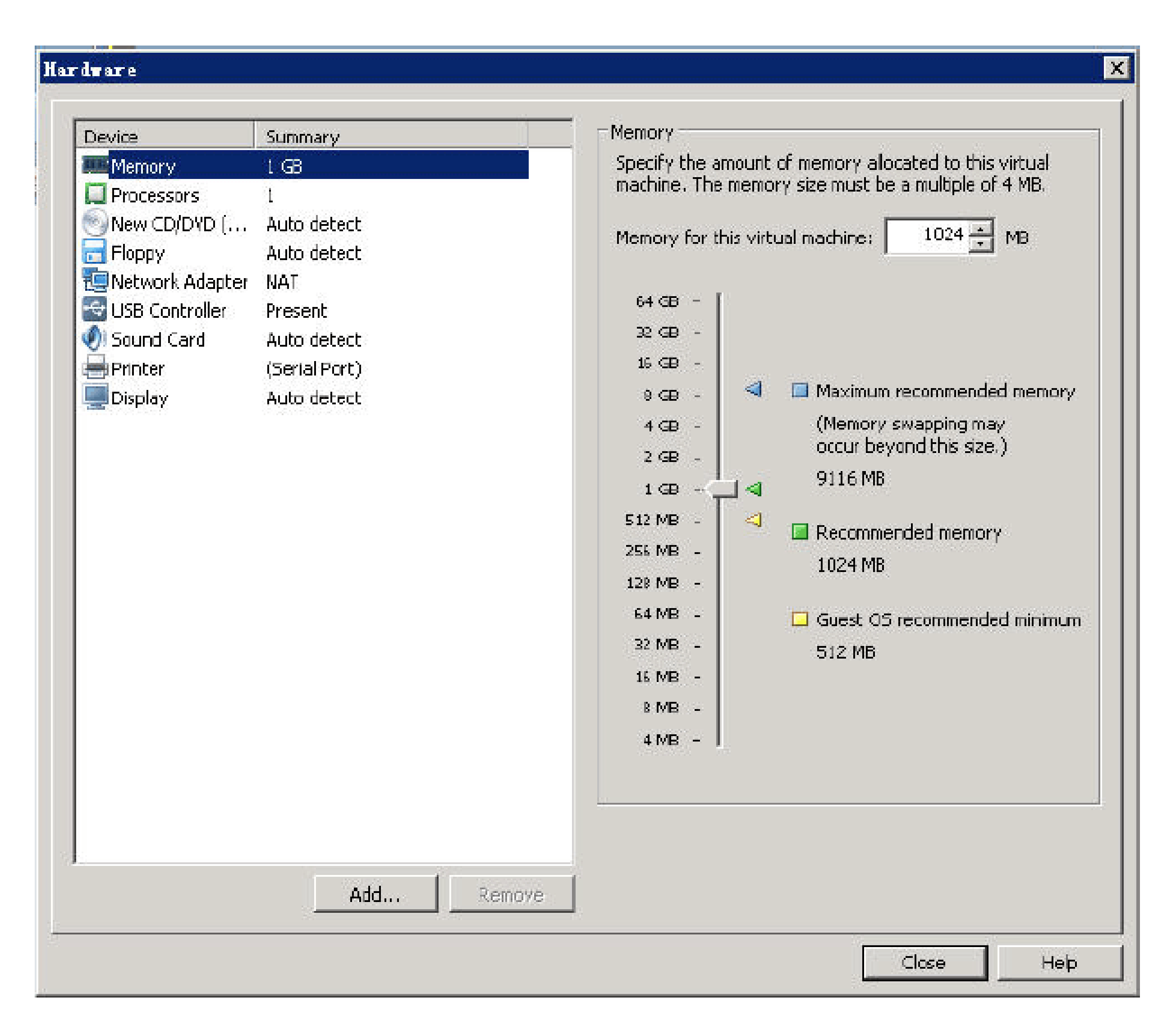
步骤06 设置硬盘容量，默认为20GB动态硬盘容量，若需要更大的硬盘容量，可根据实际硬盘容量设置，但不要超过实体硬盘的可用空间，按【Next】。



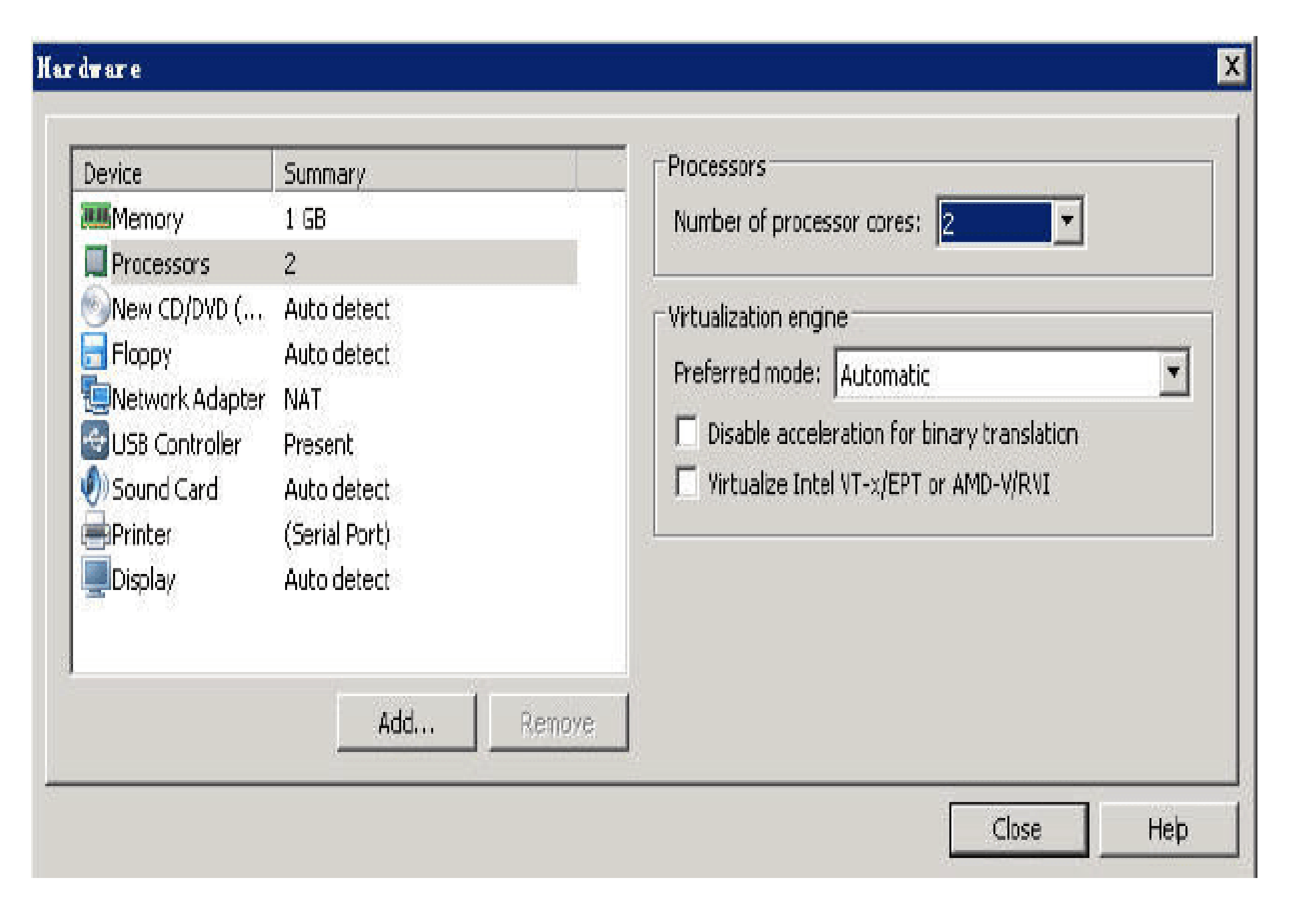

步骤07 虚拟机大致创建完成，接下来配置虚拟机，按【Customize Hardware】。



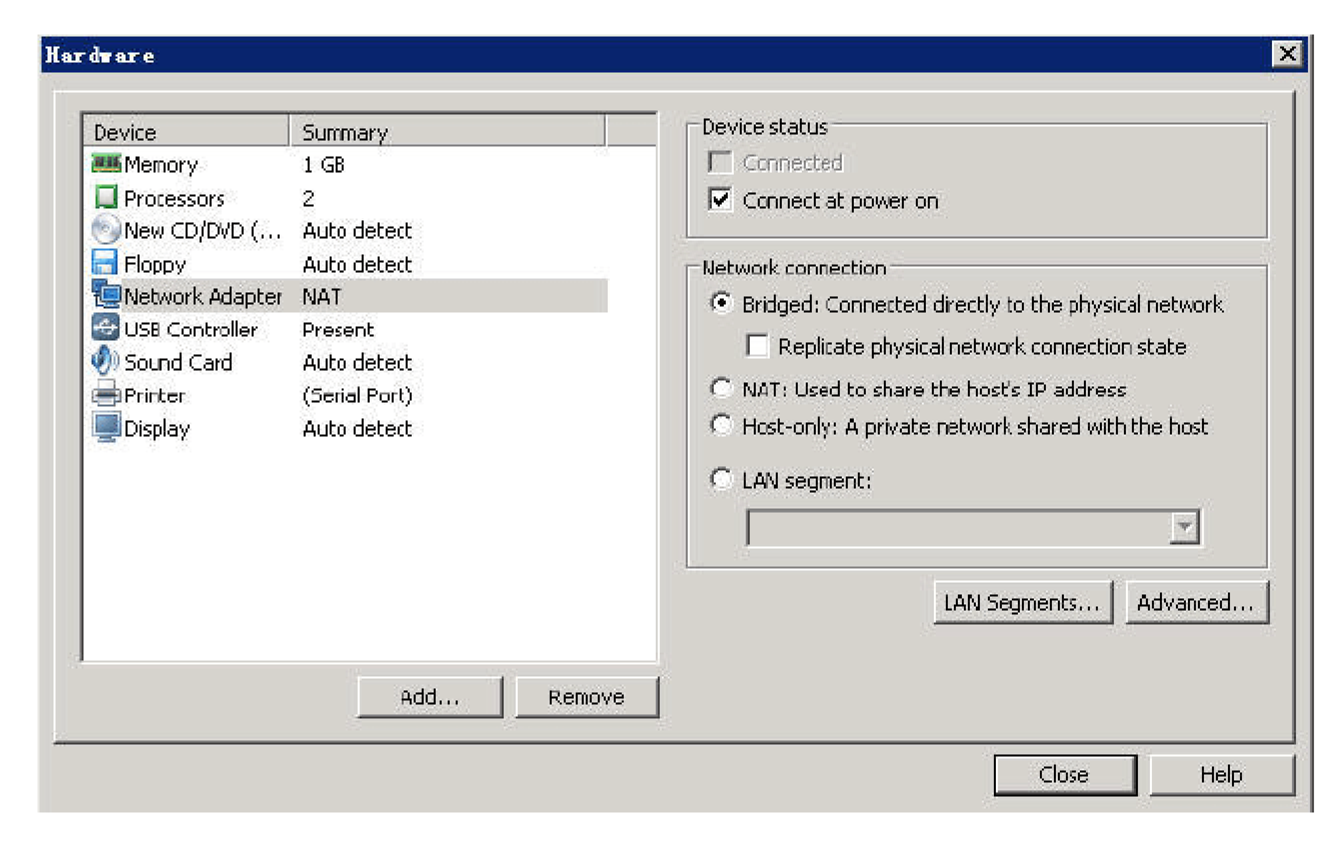

步骤08 对于内存，CentOS 6.x操作系统建议设置1GB以上，除了安装图形界面时需要较大的内存外，如果操作系统已安装图形界面，那就有需要1GB左右的内存，否则无法安装成功，若没有安装图形界面，可以在操作系统安装完毕后，再将内存容量修改为1GB以下。




步骤09 CPU处理器部分，可以根据需求设置，操作系统至少需要一个处理器。

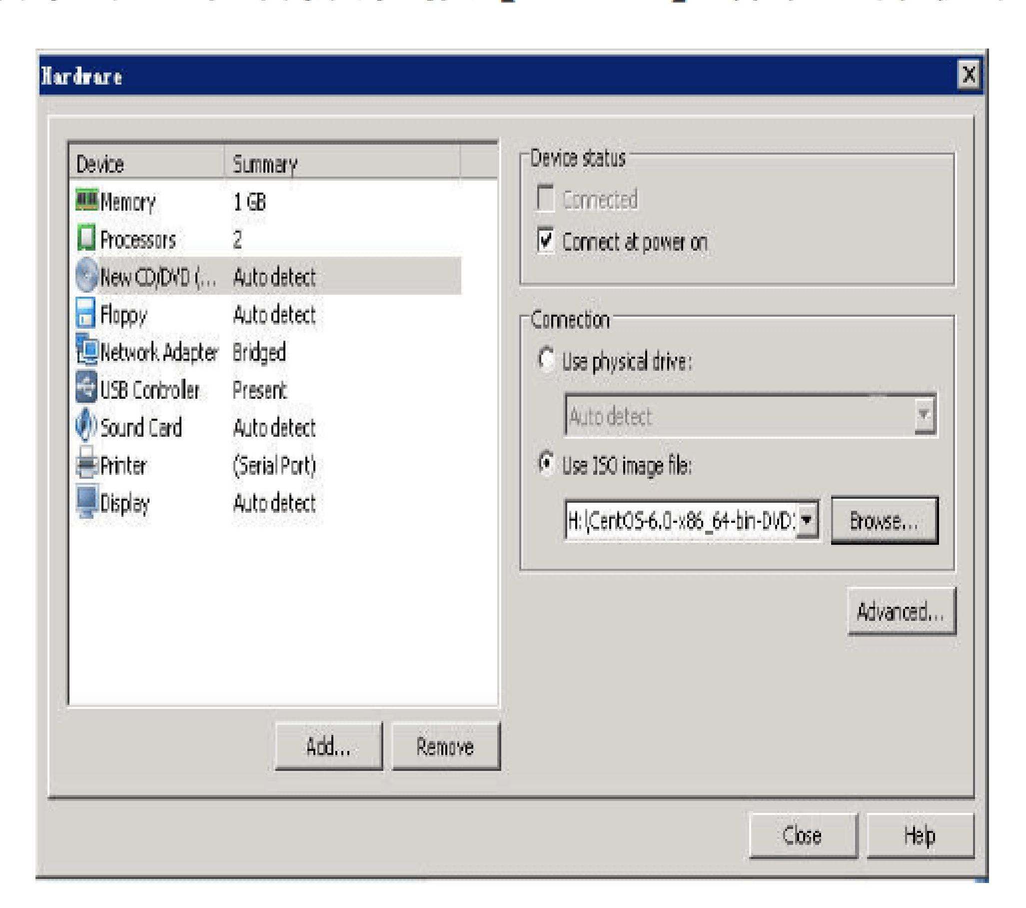



步骤10 网络部分，默认为NAT模式，对外服务就要经过比较多的设置，所以建议使用Bridged模式，这样就如同与实体主机使用同一张网卡，对外服务也较方便。

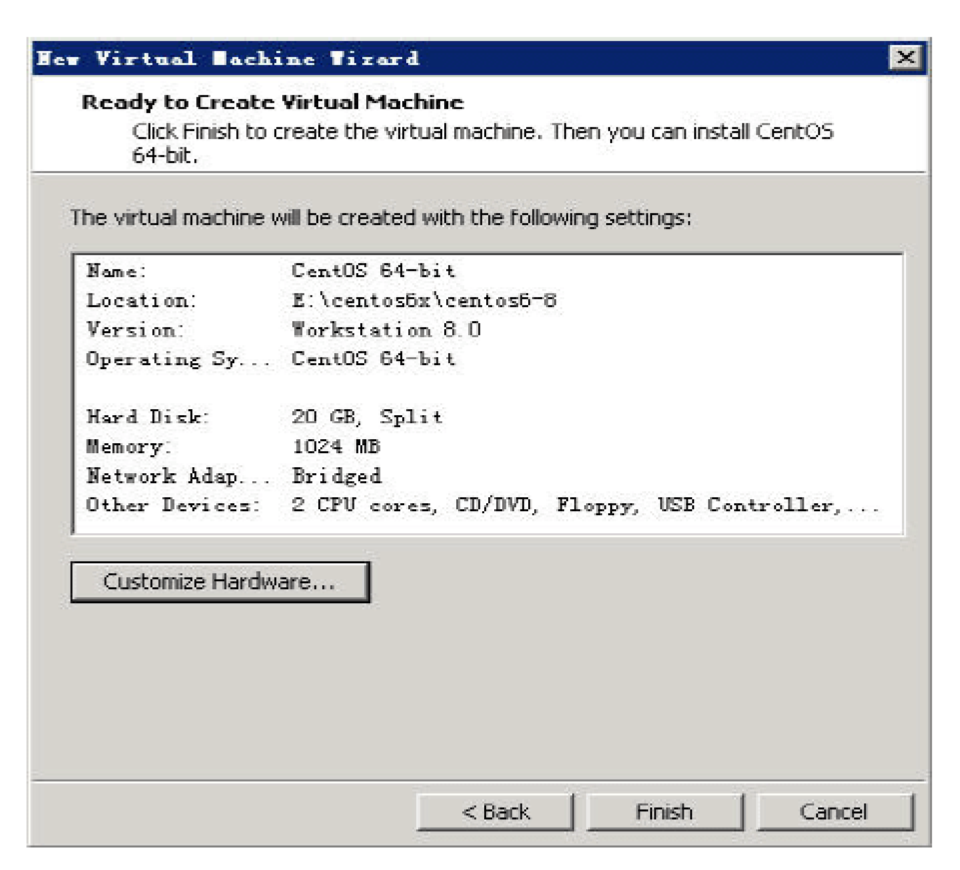



步骤11 内存、处理器、网络设置完成后，就要设置安装来源，建议使用ISO安装，其

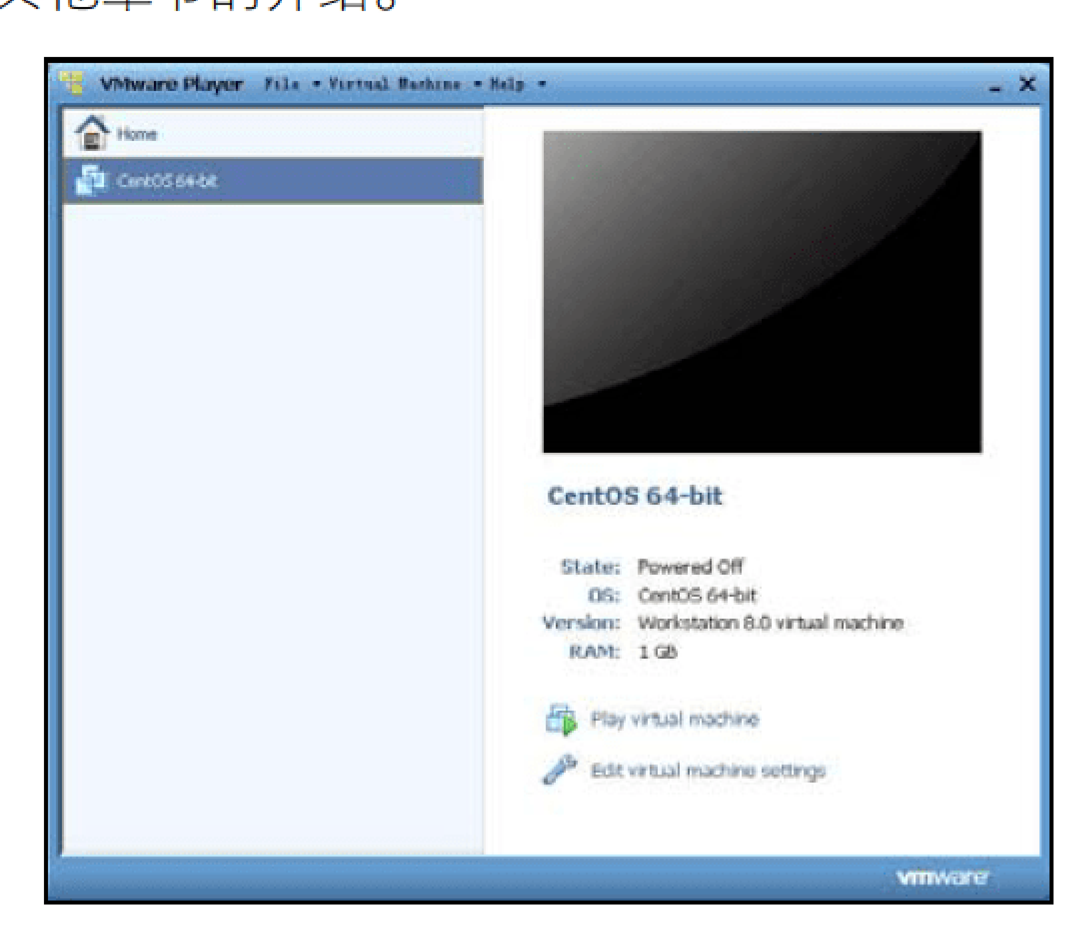
安装速度比光驱快，选择【Use ISO image file】，然后选择CentOS 6.x操作系统的ISO文件，设置完成后，按【Close】结束虚拟机设置。




步骤12 虚拟机设置完成后，按【Finish】结束设置，VMware Player就会建立虚拟机。




步骤13 在VMware Player 4窗口中可以看到刚建立的虚拟机，接下来按【Play virtual machine】，启动虚拟机，就可以开始安装CentOS操作系统了，有关安装步骤，请参见其他章节的介绍。



# 附录 B

# 使用Fedora LiveUSB Creator创建USB随身系统盘

Fedora LiveUSB Creator官方网站：https://fedorahosted.org/liveusb-creator/。

Fedora LiveUSB Creator是一款免费制作USB 随身系统盘的软件，可以将Linux提供的Live CD制作到USB上，这样不仅可以省去光盘，也提高了访问速度，更重要的是生成的数据也可以写入USB中，只要计算机支持USB开机，就可以使用此软件创建的USB 随身系统盘，笔者介绍它的目的就是要让使用者在任何地方都可以马上练习使用CentOS系统，不用一步一步将环境设置好再练习。

## 下载Fedora LiveUSB Creator软件

目前最新版本为3.11.1版本，请到官方网站下载。

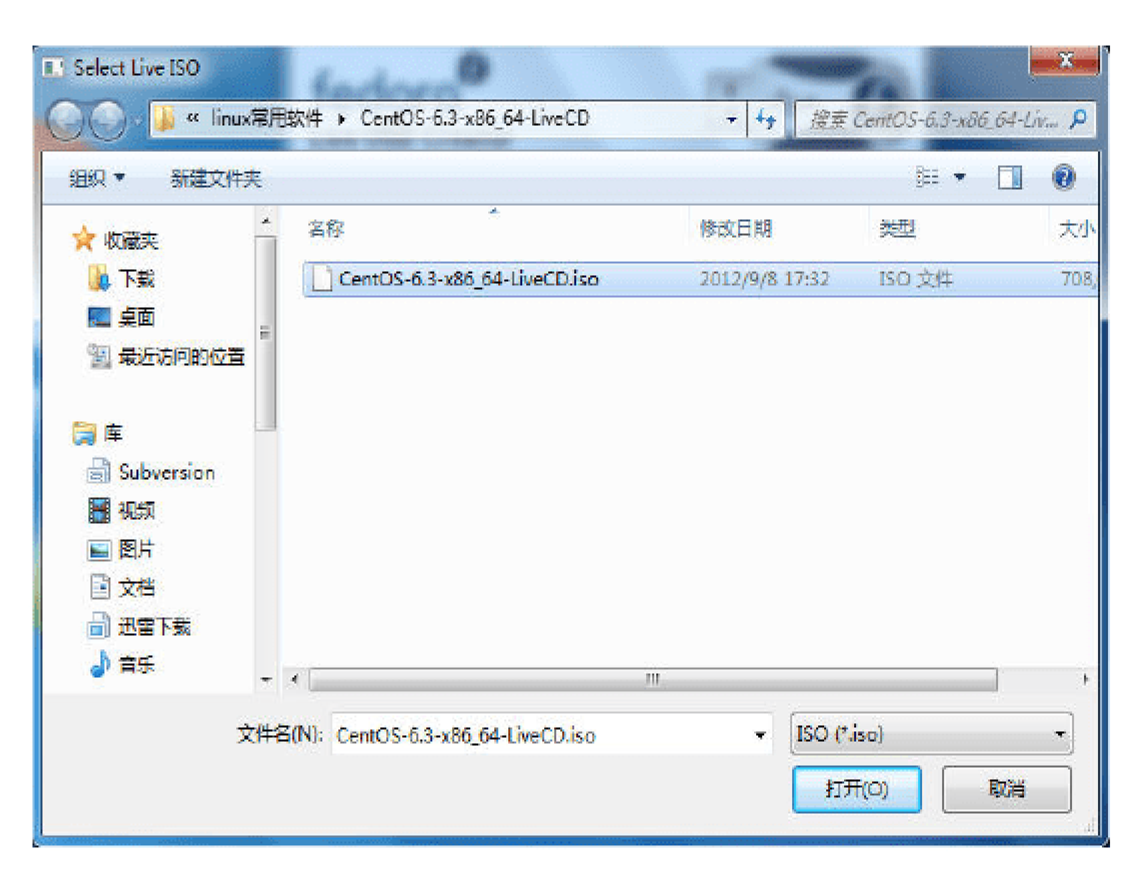
https://fedorahosted.org/releases/l/i/liveusb-creator/liveusb-creator-3.11.1-setup.exe

## Live Linux USB的制作

打开Fedora LiveUSB Creator后，制作数据源有两种方法，一种是使用Browse选项抓取已经存在的Live CD ISO，另一种就是使用Download Fedora选项下载Fedora Live CD ISO，建议使用Browse选项抓取已经存在的Live CD ISO，这样比较节省下载时间，毕竟Fedora LiveUSB Creator下载需要很长的时间，若遇到要制作多个USB，就会很浪费带宽，Live CD ISO容量为六百多兆，还可以自行创建其他版本的Linux，如CentOS、Redhat、ubuntu、openSUSE等，这里使用CentOS-6.3-x86_64-LiveCD.iso制作USB。




按【Browse】后，选择已准备好的系统ISO文件【CentOS-6.3-x86_64-LiveCD.iso】，然后按【打开】。




**说明**

Live CD一定要是CD版，不可以是DVD版本，否则制作完成也无法开机。

选择CentOS-6.3-x86_64-LiveCD.iso后，在【Target Device】中选择所要写入的USB驱动号，这里选择I磁盘这个USB驱动号，一切就绪后，按【Create Live USB】开始制作。



CentOS的Live CD要制作成USB大约需要10分钟的时间，实际速度依赖于实际环境，如下图所示，制作USB完成后，可以找一台计算机测试可不可以开机进入系统，记得要选择USB-Floppy或USB HDD开机，否则会无法开机成功。



# 附录 C

# 使用UNetbootin创建USB随身系统盘

UNetbootin官方网站：http://unetbootin.sourceforge.net/。

UNetbootin是一款免费制作USB随身Linux系统盘的软件，可以将Linux提供的Live CD制作到USB上，这样不仅可以省去光盘，访问速度也比较快，更重要的是生成的数据也可以写入到USB随身Linux系统盘中，只要计算机支持USB开机，就可以使用此软件创建的USB随身Linux系统盘，UNetbootin支持的版本也有多种，笔者介绍它的目的就是要让使用者在任何地方都可以马上使用CentOS操作系统，不用一步一步将环境设置好。

## UNetbootin软件下载

目前最新版本为563版本，请到官方网站下载。

下载地址为http://ncu.dl.sourceforge.net/project/unetbootin/UNetbootin/563/unetbootin-windows-563.exe。

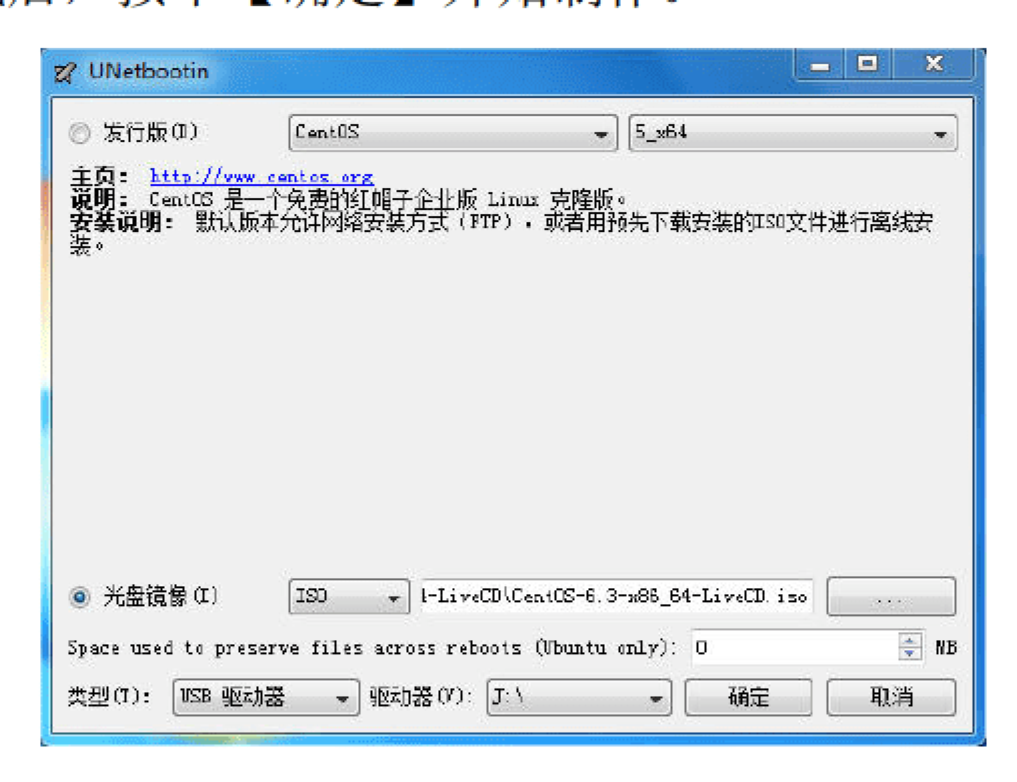
## 支持的Linux系统列表

下表为UNetbootin所支持的Linux操作系统版本，最新版本可以参考官方网站：

| Linux 名称 | 版本 |
| --- | --- |
| Ubuntu（http://www.ubuntu.com） | 8.04 LTS、8.10、9.04、9.10、10.4、10.11、11.4、11.10 |
| Debian（http://www.debian.org） | Stable/Lenny、Testing/Squeeze、Unstable/Sid |
| openSUSE（http://www.opensuse.org） | 10.2、10.3、11.0、11.1 |
| FreeBSD（http://www.freebsd.org） | 6.3、7.0、7.2、8.0 |
| Fedora（http://fedoraproject.org） | 10、11、12、13、14、15 |
| CentOS（http://www.centos.org） | 4、5 |
| Mandriva（http://www.mandriva.com/） | 2007.1、2008.0、2008.1 |

## 制作Live Linux USB的步骤

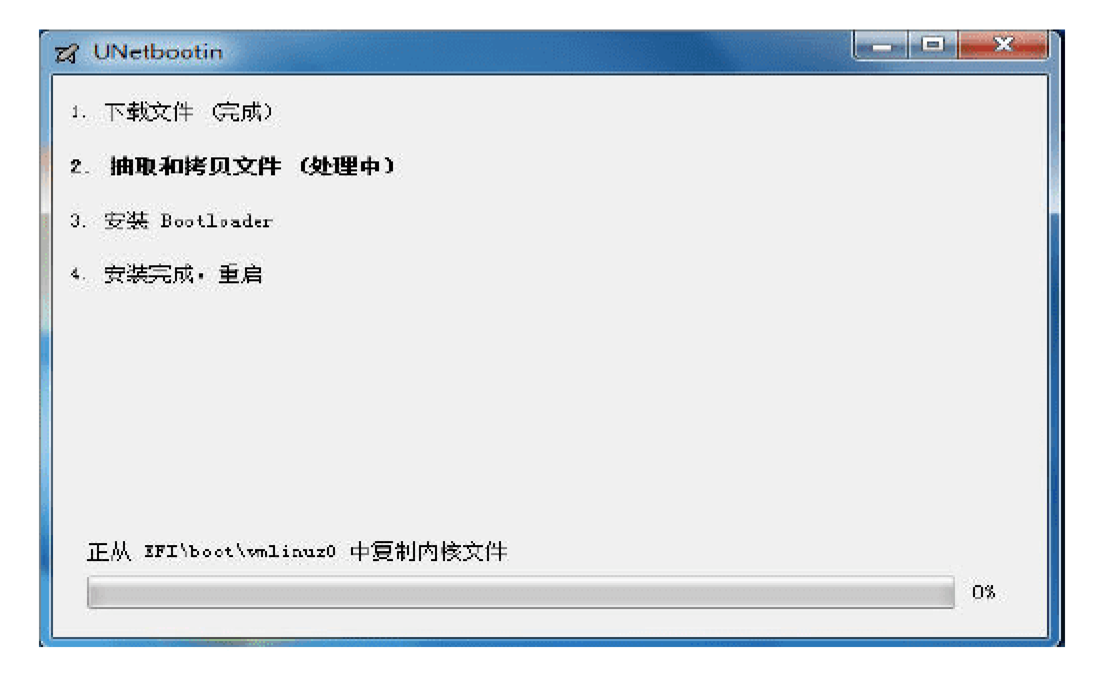
UNetbootin可以通过镜像网站提取发行版本文件，软件会自动下载制作，此方式比较耗时、制作成功率不高，另一种方式是在映像文件中读取Live CD ISO文件，如下图所示，此方式比较稳定快速，选取好ISO文件后，【类型】选择【USB驱动器】，【驱动器】选择所要写入的USB驱动号，设置完成后，按下【确定】开始制作。



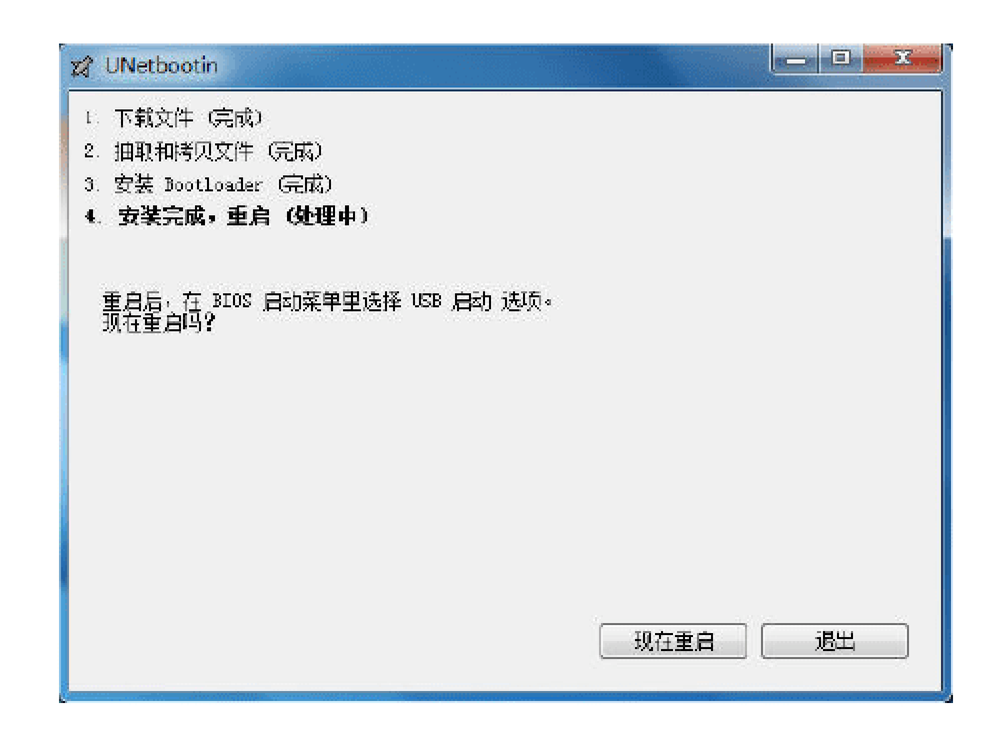

说明

Live Linux USB一定要是CD版，不可以是DVD版本，否则制作完成也无法开机。

制作Live Linux USB大约需要10分钟的时间，所用的时间取决于实际环境。




制作完成后，可以立即重新启动进行测试，记得要选择USB- Floppy或USB HDD开机，否则无法开机成功。



# 附录 D

## 文件权限列表

| 所属人员 | 文件形态 | 所有者（u） | | | 所属组（g） | | | 其他用户（o） | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 操作 | d | 读取 | 写入 | 执行 | 读取 | 写入 | 执行 | 读取 | 写入 | 执行 |
| 权限 | - | r | w | x | r | w | x | r | w | x |
| 数字 | l、b、c | 4 | 2 | 1 | 4 | 2 | 1 | 4 | 2 | 1 |

| 文件形态 | 文件形态说明 |
|---|---|
| d | 目录 |
| - | 文件 |
| l | 链接文件 |
| b | 块设备文件 |
| c | 字符设备文件 |

| 权限数字 | 数字相加 | 权限表示 |
|---|---|---|
| 0 | 0+0+0 | - - - |
| 1 | 0+0+1 | - - x |
| 2 | 0+2+0 | - w - |
| 3 | 0+2+1 | - w x |
| 4 | 4+0+0 | r - - |
| 5 | 4+0+1 | r – x |
| 6 | 4+2+0 | r w - |
| 7 | 4+2+1 | r w x |

| 权限 | 权限说明 |
|---|---|
| r | 可以读取文件或目录内容 |
| w | 可以创建、修改、删除文件或目录 |
| x | 可以执行 |
| - | 无权限 |

| 所属人员 | 权限类型 | 权限表示法一 | 权限表示法二 |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 所有者（u） | 读取 | u=r | u+r |
| | 读取+写入 | u=rw | u+w |
| | 读取+执行 | u=rx | u+x-r |
| | 写入+执行 | u=wx | u+x-w |
| | 读取+写入+执行 | u=rwx | u+x |
| 所属组（g） | 读取 | g=r | g+r |
| | 读取+写入 | g=rw | g+w |
| | 读取+执行 | g=rx | g+x-r |
| | 写入+执行 | g=wx | g+x-w |
| | 读取+写入+执行 | g=rwx | g+x |
| 其他用户（o） | 读取 | o=r | o+r |
| | 读取+写入 | o=rw | o+w |
| | 读取+执行 | o=rx | o+x-r |
| | 写入+执行 | o=wx | o+x-w |
| | 读取+写入+执行 | o=rwx | o+x |
| 所有用户（a） | 读取 | a=r | a+r |
| | 读取+写入 | a=rw | a+w |
| | 读取+执行 | a=rx | a+x-r |
| | 写入+执行 | a=wx | a+x-w |
| | 读取+写入+执行 | a=rwx | a+x |

说明

若同时设置两个所属人员必须以逗号区分，例如u=rwx,o=wx。

| 运算符 | 说明 |
|---|---|
| = | 权限设置 |
| + | 权限增加 |
| - | 权限减少 |

说明

若原来所有者权限为rwx，要将写入权限删除，可以使用权限表示法二的操作，就必须要使用运算符“–”删除权限，如【u-w】。




# cron计划任务

crontab命令常见于Unix和类Unix的操作系统之中，用于设置计划执行命令。

## cron服务

| 命令 | 命令说明 |
|---|---|
| service crond start | 启动服务 |
| service crond stop | 关闭服务 |
| service crond restart | 重启服务 |
| service crond reload | 重载服务 |

## corn参数设置

| 命令参数 | 参数说明 |
|---|---|
| crontab -u | 设置用户的 cron 服务 |
| crontab -l | 列出 cron 服务的详细内容 |
| crontab -r | 删除 cron 服务 |
| crontab -e | 编辑 cron 服务 |

说明

通常不设置使用者，默认为root。

## corn时间设置

| 时间 | 时间范围 |
|---|---|
| 分钟 | 0~59 |
| 小时 | 0~23 |

（续表）

| 时间 | 时间范围 |
|---|---|
| 日期 | 1~31 |
| 月份 | 1~12 |
| 星期 | 0~6（0 为星期天） |
| ,逗号 | 代表多个时间段，例如 3 点和 6 点为 3,6 |
| *星号 | 代表所有时间 |
| -减号 | 代表每个时间段，例如 1 点到 3 点为 1-3 |
| /斜线 | 代表每隔多久，如果每两个小时要执行一次，则为*/2 |

输入【crontab -e】，例如：

每天中午12点 30 分执行/tmp/test.sh。

```
30 12 * * *   /tmp/test.sh
```

每个月1号1点至3点30分执行/tmp/test.sh。

```
30 1-3 1 * *   /tmp/test.sh
```

每年的7月7号17点20分执行/tmp/test.sh

```
20 17 7 7 *    /tmp/test.sh
```

每个星期天每过30分执行/tmp/test.sh

```
*/30 * * * 0   /tmp/test.sh
```

# 附录 F

# YUM在线更新命令

| 更新/升级 update/upgrade | |
|---|---|
| **命令** | **命令说明** |
| yum check-update | 列出所有可更新的软件清单 |
| yum update | 更新系统已安装软件 |
| yum upgrade | 升级软件，连一些过旧即将淘汰的软件也会一并升级 |

| 安装/删除/搜索 install/remove/search | |
|---|---|
| **命令** | **命令说明** |
| yum install <package_name> | 安装指定的软件 |
| yum remove <package_name> | 删除指定的软件 |
| yum search <keyword> | 搜索软件 |

| 清除 clean | |
|---|---|
| **命令** | **命令说明** |
| yum clean packages | 清除缓存目录（/var/cache/yum）下的软件 |
| yum clean headers | 清除缓存目录（/var/cache/yum）下的 headers |
| yum clean oldheaders | 清除缓存目录（/var/cache/yum）下旧的 headers |
| yum clean all（= yum clean packages; yum clean oldheaders） | 清除缓存目录（/var/cache/yum）下的软件及旧的 headers |
| yum clean cache | 清除缓存目录（/var/cache/yum）下的 cache |
| yum clean metadata | 清除缓存目录（/var/cache/yum）下的 metadata |

| 列表 list | |
|---|---|
| 命令 | 命令说明 |
| yum list | 列出所有可安装的软件 |
| yum list updates | 列出所有可更新的软件 |
| yum list installed | 列出所有已安装的软件 |
| yum list extras | 列出所有已安装但不在 Yum Repository 内的软件 |
| yum list <package_name> | 列出所指定的软件 |

| 软件组 group | |
|---|---|
| 命令 | 命令说明 |
| yum grouplist | 列出所有可安装的软件组 |
| yum groupinstall | 安装软件组 |
| yum groupupdate | 更新软件组 |
| yum groupremove | 删除软件组 |
| yum groupinfo | 列出软件组信息 |

| 信息 info | |
|---|---|
| 命令 | 命令说明 |
| yum info | 列出所有软件的信息 |
| yum info updates | 列出所有可更新的软件信息 |
| yum info installed | 列出所有已安装的软件信息 |
| yum info extras | 列出所有已安装但不在 Yum Repository 内的软件信息 |
| yum info <package_name> | 列出所指定的软件信息 |
| yum provides <package_name> | 列出软件提供哪些文件 |